Performance and Accountability Report

Fiscal Year 2005

Management's Discussion and Analysis

Part I

U.S. Department of Homeland Security

Homeland Security

The Department at a Glance

Vision

Preserving our freedoms, protecting America…
we secure our homeland.

HISTORY

Guided by the National Strategy for Homeland Security and the Homeland Security Act of 2002, the President signed an Executive Order in January 2003 establishing the nation's 15th Cabinet agency, the Department of Homeland Security. The purpose of the new Department, which incorporated 180,000 employees from 22 organizations, is to provide the unifying core for the vast national network of organizations and institutions involved in securing the nation from terrorist threats and natural disasters. In less than three years of operation, the Department has achieved many important operational and policy objectives.

MISSION

We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. We will ensure safe and secure borders, welcome lawful immigrants and visitors, and promote the free flow of commerce.

STRATEGIC GOALS

Awareness — Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.

Prevention — Detect, deter and mitigate threats to our homeland.

Protection — Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters, or other emergencies.

Response — Lead, manage and coordinate the national response to acts of terrorism, natural disasters, or other emergencies.

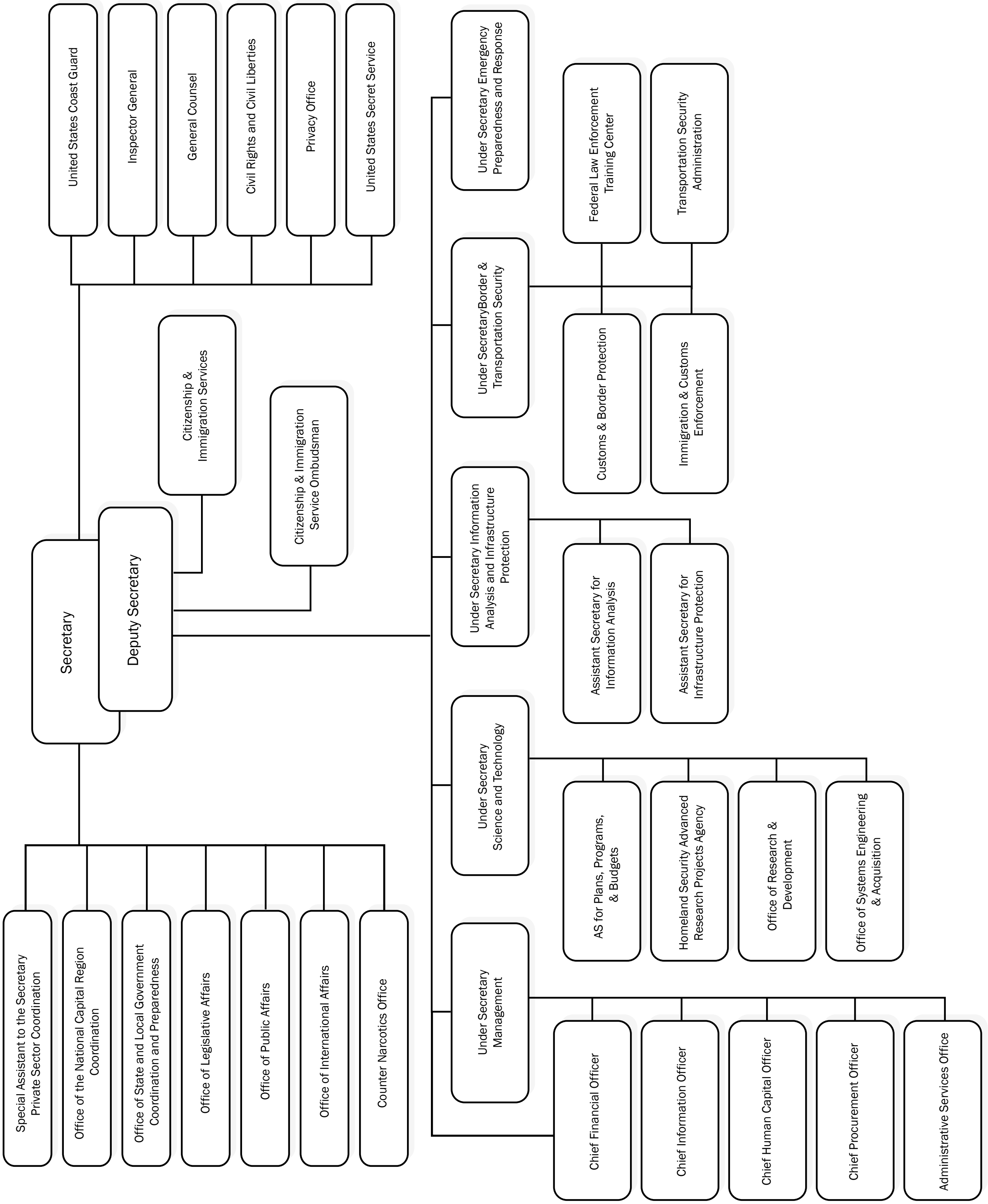
Recovery — Lead national, state, local and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies.

Service — Serve the public effectively by facilitating lawful trade, travel and immigration.

Organizational Excellence — Value our most important resource, our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability and teamwork to achieve efficiencies, effectiveness, and operational synergies.

ORGANIZATION

To accomplish our goals, we were organized as follows in fiscal year 2005:


United States Coast Guard
Inspector General
General Counsel
Civil Rights and Civil Liberties
Privacy Office
United States Secret Service
Citizenship & Immigration Services
Citizenship & Immigration Service Ombudsman
Secretary
Deputy Secretary
Special Assistant to the Secretary Private Sector Coordination
Office of the National Capital Region Coordination
Office of State and Local Government Coordination and Preparedness
Office of Legislative Affairs
Office of Public Affairs
Office of International Affairs
Counter Narcotics Office
Under Secretary Emergency Preparedness and Response
Under SecretaryBorder & Transportation Security
Federal Law Enforcement Training Center
Transportation Security Administration
Customs & Border Protection
Immigration & Customs Enforcement
Under Secretary Information Analysis and Infrastructure Protection
Assistant Secretary for Information Analysis
Assistant Secretary for Infrastructure Protection
Under Secretary Science and Technology
AS for Plans, Programs, & Budgets
Homeland Security Advanced Research Projects Agency
Office of Research & Development
Office of Systems Engineering & Acquisition
Under Secretary Management
Chief Financial Officer
Chief Information Officer
Chief Human Capital Officer
Chief Procurement Officer
Administrative Services Office

To accomplish its mission, the Department in fiscal year 2005 was organized into five directorates and several components:

DIRECTORATES

1. **The Information Analysis and Infrastructure Protection (IAIP) Directorate** identifies and assesses a broad range of intelligence information concerning threats to the Homeland, issues timely warnings, and takes appropriate preventive and protective action. The Directorate has two essential functions:

   - **Information Analysis** provides actionable intelligence essential for preventing acts of terrorism and, with timely and thorough analysis and dissemination of information about terrorists and their activities, improves the Federal government's ability to disrupt and prevent terrorist acts and to provide useful warning to state and local governments, the private sector and our citizens; and

   - **Infrastructure Protection** coordinates national efforts to secure America's critical infrastructure, including vulnerability assessments, strategic planning efforts and exercises. Protecting America's critical infrastructure is the shared responsibility of the Federal government and state and local governments in active partnership with the private sector, which owns approximately 85 percent of the nation's critical infrastructure.

2. The **Border and Transportation Security (BTS) Directorate** ensures the security of the nation's borders and transportation systems. Its first priority is to prevent the entry of terrorists and the instruments of terrorism while simultaneously ensuring the efficient flow of lawful traffic and commerce. BTS manages and coordinates port-of-entry activities and leads efforts to create borders that are more secure as a result of better intelligence, coordinated national efforts and unprecedented international cooperation against terrorists, the instruments of terrorism and other international threats. BTS includes the following components:

   - The **U.S. Customs and Border Protection (CBP)** provides security at America's borders and ports of entry, as well as extends our zone of security beyond our physical borders. This ensures that American borders are the last line of defense, not the first. CBP is also responsible for processing all people, vehicles and cargo entering the United States; apprehending individuals attempting to enter the United States illegally; stemming the flow of illegal drugs and other contraband; protecting our agricultural and economic interests from harmful pests and diseases; regulating and facilitating international trade and travel; protecting American businesses from theft of intellectual property and unfair trade practices; collecting import duties; maintaining export controls; and enforcing U.S. trade laws.

   - The **U.S. Immigration and Customs Enforcement (ICE)**, the largest investigative arm of the Department, enforces Federal immigration, customs and air security laws. ICE also provides protection and security for Federal Government buildings. ICE's primary mission is to detect vulnerabilities and prevent violations that threaten national security. ICE works to protect the

United States and its people by deterring, interdicting and investigating threats arising from the movement of people and goods into and out of the United States, and by policing and securing Federal facilities across the nation.

- The **Transportation Security Administration (TSA)** protects the nation's transportation systems to ensure freedom of movement for people and commerce. TSA will continuously set the standard for excellence in transportation security through its people, processes and technologies.
- The **Federal Law Enforcement Training Center (FLETC)**, the Federal government's leader for and provider of world-class law enforcement training, prepares new and experienced law enforcement professionals to fulfill their responsibilities safely and at the highest level of proficiency. FLETC provides training in the most cost-effective manner.

3. The **Emergency Preparedness and Response (EP&R) Directorate** ensures that the nation is prepared for, and able to recover from, terrorist attacks and natural disasters. The Directorate provides domestic disaster preparedness training and coordinates government disaster response. The core of emergency preparedness includes the Federal Emergency Management Agency (FEMA), which is responsible for reducing the loss of life and property and protecting the nation's institutions from all types of hazards through a comprehensive emergency management program of preparedness, prevention, response and recovery.

4. The **Science and Technology (S&T) Directorate** provides Federal, state and local operators with the technology and capabilities needed to protect the nation from catastrophic terrorist attacks, including threats from weapons of mass destruction. S&T will develop and deploy state-of-the-art, high-performing, low-operating-cost systems to detect and rapidly mitigate the consequences of terrorist attacks, including attacks that may use chemical, biological, radiological and nuclear materials.

5. The **Management Directorate** oversees the budget; appropriations; expenditure of funds; accounting and finance; procurement; human resources and personnel; information technology systems; facilities, property, equipment and other material resources; program performance planning; and identification and tracking of performance measures aligned with the Department's mission. The Chief Financial Officer (CFO), Chief Information Officer (CIO), Chief Human Capital Officer (CHCO), Chief Procurement Officer (CPO) and Chief of Administrative Services (CAO) are within the Management Directorate. The CFO and CIO also report directly to the Secretary of Homeland Security.

COMPONENTS

In addition to the five major directorates, the Department includes other critical components:

The **Office of the Secretary** includes components that share a direct reporting structure to the Secretary and Deputy Secretary. Some of these components include the Offices of the General Counsel, Civil Rights and Civil Liberties, Legislative Affairs, Public Affairs and International Affairs, as well as the Privacy Office and Counter Narcotics Office.

The **U.S. Coast Guard (USCG)** ensures maritime safety, mobility and security, protects our natural marine resources and provides national defense as one of the five U.S. armed services. Its mission is to protect the public, the environment and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support our national security. The USCG also prevents maritime terrorist attacks, halts the flow of illegal drugs and contraband, prevents individuals from entering the United States illegally, and prevents illegal incursion in our Exclusive Economic Zone. Upon declaration of war, or when the President so directs, USCG will operate as an element of the Department of Defense, consistent with existing law.

The **U.S. Secret Service (Secret Service)** protects the President and Vice President, their families, heads of state and other designated individuals; investigates threats against these individuals; protects designated facilities; and plans and implements security for designated national special security events. The Secret Service also investigates violations of laws relating to counterfeiting and financial crimes, including computer fraud and computer-based attacks on the nation's financial, banking and telecommunications infrastructure

The **U.S. Citizenship and Immigration Services (USCIS)** directs the nation's immigration benefit system and promotes citizenship values by providing immigration services such as immigrant and non-immigrant sponsorship; adjustment of status; work authorization and other permits; naturalization of qualified applicants for U.S. citizenship; and asylum or refugee processing. USCIS makes certain that America continues to welcome visitors and those who seek opportunity within our shores while excluding terrorists and their supporters.

The **Office of State and Local Government Coordination and Preparedness (SLGCP)** serves as a single point of contact for facilitation and coordination of departmental programs that impact state, local, territorial and tribal governments. The Department has brought together many organizations with a long history of interaction with, and support to, state, local, territorial and tribal government organizations and associations, and the office is working hard to consolidate and coordinate that support.

The **Office of Inspector General (OIG)** serves as an independent and objective inspection, audit and investigative body to promote effectiveness, efficiency and economy in the Department's programs and operations. OIG seeks to prevent and detect fraud, abuse, mismanagement and waste.

Some of the things the men and women of the Department of Homeland Security do on an average day are listed below.

- Process more than 1.1 million passengers and pedestrians, 365,079 vehicles, and 64,432 tuck, rail, and sea containers through our ports of entry.
- Seize 4,224 prohibited plant materials or animal products at our ports of entry.
- Screen approximately 1.8 million domestic and international passengers -- each carrying an average of two bags -- before they board commercial aircraft.
- Intercept more than 36,600 prohibited items at airports -- including two firearms -- each day.

- Assist 117 people in distress at sea, interdict 30 illegal migrants, conduct 90 search and rescue, and board and inspect 122 vessels in the maritime environment.
- Respond to 11 oil and hazardous chemical spills in the maritime environment.
- Conduct 135,000 national security background checks, process 30,000 applications for immigrant benefits, and issue 7,000 Permanent Resident Cards (green cards).
- Welcome 2,100 new citizens, 3,500 new permanent residents, and nearly 200 refugees from around the world.
- Grant asylum to 80 individuals already in the United States, naturalize 20 individuals serving in the U.S. military and help American parents adopt nearly 80 foreign-born orphans.
- Provide weapons of mass destruction (WMD) training to 175 first responders to improve their capacity to prevent, protect against, respond to, and recover from acts of terrorism and other disasters.
- Provide law enforcement training to approximately 2,240 law enforcement officers and agents from 82 Partner Organizations.

Reorganization Note: Based on the Department's Second Stage Review, the Department proposed realigning the Department of Homeland Security to increase its ability to prepare, prevent and respond to terrorist attacks and other emergencies. These changes will better integrate the Department and give its employees better tools to accomplish their mission. As a result of this realignment, certain organizational changes will take effect in fiscal year 2006.

A six-point agenda will guide the Department in the near term and result in changes that will:

1. Increase overall preparedness, particularly for catastrophic events;
2. Create better transportation security systems to move people and cargo more securely and efficiently;
3. Strengthen border security and interior enforcement and reform immigration processes;
4. Enhance information sharing with our partners;
5. Improve the Department's financial management, human resource development, procurement, and information technology; and
6. Realign the Department's organization to maximize mission performance.

ORGANIZATIONAL INITIATIVES: STRUCTURAL ADJUSTMENTS

Supporting the agenda, the Secretary proposes to realign the Department to increase its ability to prepare, prevent, and respond to terrorist attacks and other emergencies. These changes will better integrate the Department and give employees better tools to accomplish their mission.

Centralize and Improve Policy Development and Coordination. The new Directorate of Policy will:

- Be the primary Department-wide coordinator for policies, regulations, and other initiatives;
- Ensure consistency of policy and regulatory development across the Department;
- Perform long-range strategic policy planning;
- Assume the policy coordination functions previously performed by the BTS Directorate; and
- Include the Office of International Affairs, Office of Private Sector Liaison, Homeland Security Advisory Council, Office of Immigration Statistics, and Senior Asylum Officer.

Strengthen Intelligence Functions and Information Sharing. A new Office of Intelligence and Analysis will ensure that information is:

- Gathered from all relevant field operations and other parts of the intelligence community;
- Analyzed with a mission-oriented focus;
- Informed to senior decision-makers; and
- Disseminated to the appropriate Federal, state, local and private-sector partners.

Led by a Chief Intelligence Officer reporting directly to the Secretary, the Office of Intelligence will be comprised of analysts within the former Information Analysis directorate and draw on the expertise of other department components with intelligence collection and analysis operations.

Improve Coordination and Efficiency of Operations. The new Director of Operations Coordination will:

- Conduct joint operations across all organizational elements;
- Coordinate incident management activities; and
- Use all resources within the Department to translate intelligence and policy into immediate action.

The Homeland Security Operations Center, which serves as the nation's nerve center for information sharing and domestic incident management on a 24/7/365 basis, will be a critical part of this new office.

Enhance Coordination and Deployment of Preparedness Assets. The Directorate for Preparedness will:

- Consolidate preparedness assets from across the Department;
- Facilitate grants and oversee nationwide preparedness efforts supporting first responder training, citizen awareness, public health, infrastructure and cyber security and ensure proper steps are taken to protect high-risk targets;
- Focus on cyber security and telecommunications; and

- Include a new Chief Medical Officer, responsible for carrying out the Department's responsibilities to coordinate the response to biological attacks.

Managed by an Under Secretary, this Directorate will include infrastructure protection; assets of SLGCP, which is responsible for grants, training and exercises; the U.S. Fire Administration; and the Office of National Capitol Region Coordination.

OTHER DEPARTMENT REALIGNMENTS

Improve National Response and Recovery Efforts by Focusing FEMA on Its Core Functions. FEMA will report directly to the Secretary. In order to strengthen and enhance the nation's ability to respond to and recover from man-made or natural disasters, FEMA will focus on its traditional and vital mission of response and recovery.

Integrate Federal Air Marshal Service (FAMS) into Broader Aviation Security Efforts. The Federal Air Marshal Service will be moved from ICE to TSA to increase operational coordination and strengthen efforts to meet the common goal of aviation security.

Merge Legislative and Intergovernmental Affairs. A new Office of Legislative and Intergovernmental Affairs will merge certain functions between the Office of Legislative Affairs and the Office of State and Local Government Coordination in order to streamline intergovernmental efforts and better share homeland security information with members of Congress as well as state and local officials.

Assign Office of Security to Management Directorate. The Office of Security will be moved to return oversight of that office to the Under Secretary for Management in order to better manage information systems, contractual activities, security accreditation, training and resources.

Implementing the President's Management Agenda

The *President's Management Agend*a (PMA) was launched in August 2001 as a strategy for improving the management and performance of the Federal government. The PMA focuses on the areas where deficiencies were most apparent and where the government could begin to deliver concrete, measurable results. The agenda includes five original PMA initiatives, and two additional government-wide initiatives.

The five original PMA initiatives are:

- **Strategic Management of Human Capital** — having processes in place to ensure the right person is in the right job, at the right time, and is not only performing, but performing well;
- **Competitive Sourcing** — regularly examining commercial activities performed by the government to determine whether it is more efficient to obtain such services from Federal employees or from the private sector;
- **Improved Financial Performance** — accurately accounting for the taxpayers' money and giving managers timely and accurate program cost information for management decisions and control costs;
- **Expanded Electronic Government** — ensuring that the Federal government investment in information technology significantly improves the government's ability to serve citizens, and that information technology systems are secure and delivered on time and on budget; and
- **Budget and Performance Integration** — ensuring that performance is routinely considered in funding and management decisions and those programs achieve expected results and work toward continual improvement. For each initiative, the PMA established clear, government-wide goals or standards for success in budget and performance integration.

The two additional PMA initiatives are:

- **Eliminating Improper Payments** – accurately identifying, preventing and eliminating erroneous payments.
- **Real Property** – assuring that the Federal government's real property assets are available; of the right size and type; safe, secure and sustainable; able to provide quality workspaces; affordable; and operate efficiently and effectively.

OMB has rated the Department's performance in each of the five critical areas and the two additional initiatives, as shown below.

PRESIDENT'S MANAGEMENT AGENDA SCORECARD

(As of September 30, 2005)

	Status FY03	Status FY04	Status FY05	Progress FY05
Human Capital	🟥	🟥	🟨	🟩
Competitive Sourcing	🟨	🟨	🟨	🟩
Financial Performance	🟥	🟥	🟥	🟨
E-Government	🟥	🟥	🟥	🟥
Budget & Performance	🟥	🟨	🟨	🟩
Eliminating Improper Payments*	□	□	🟥	🟩
Real Property*	□	🟥	🟥	🟩

* Program-Specific Initiatives
Eliminating Improper Payments is new for FY 2005. It replaces R&D Investment Criteria reported in the Department's FY 2004 Performance and Accountability Report.

Under each standard, an agency is "**green**" if it meets all of the standards for success, "yellow" if it has achieved some but not all of the criteria and "red" if it has one or more serious flaws.

Each year the standards for green become more demanding. Despite higher fiscal year 2005 standards, the Department of Homeland Security attained green progress scores in five of seven areas.

The following is a summary of the Department's accomplishments by area for fiscal year 2005.

ENHANCED STRATEGIC MANAGEMENT OF HUMAN CAPITAL

- The Department's new Human Resources Management System, MAXHR, links individual performance to strategic goals and better rewards top performers. We also initiated standardized leadership development training, implemented a new performance appraisal system for the Senior Executive Service (SES), and completed a mapping and assessment of the Department's current hiring process to enable improved competition.
- We developed a SES/Senior Leader Candidate Development Program, identified common core business processes to enable shared services and prototyped a Department-wide Human Re-

INCREASED COMPETITIVE SOURCING

- The Department continues to improve the quality and quantity of its law enforcement mission capability by expanding implementation of the PMA Competitive Sourcing Initiative. As part of the 2005 Department of Homeland Security Federal Activities Inventory Reform (FAIR) Act (P.L.105 270), inventories of governmental functions were identified as performing commercial activities that could be performed under a competitively awarded contract or reimbursable agreement with another agency. This has required managers and employees to focus on the Department's mission and to commit to protecting the nation by using all of our available resources in the most efficient manner possible and without regard to historical approaches or a culture of reliance on in-house resources.
- The Department has completed 12 competitions involving 362 full-time employees (FTE). Our plan to get to a green rating includes completing studies involving 1,811 FTE in fiscal year 2006 and more than 3,000 FTE each year thereafter.
- The Department is coordinating its Competitive Sourcing plans with its Work Force Planning requirements to help mitigate the adverse impacts of emerging skill gaps, and hiring and training costs, and to minimize the adverse impacts on employees that may be caused by a full and open competition for the performance of commercial work.

IMPROVED FINANCIAL PERFORMANCE

This year, the Department initiated the CFO's Three Year Vision for Department of Homeland Security Financial Reporting. The theme for fiscal year 2005 was "Full Visibility and Corrective Actions." The goals for fiscal year 2005 were to: (1) submit the *Fiscal Year 2005 Performance and Accountability Report* on time, (2) receive a qualified balance sheet opinion, (3) reduce the number of material weaknesses, and (4) prepare a Secretary's Assertion on Internal Controls over Financial Reporting. The Department successfully met goals 1 and 4. It is noteworthy that separate, stand-alone audits at TSA and CBP successfully supported the Department's goals. At the consolidated level, goals 2 and 3 were not met. Material weaknesses at several components prevented the auditors from completing the testing necessary to support an overall opinion on the Department's fiscal year 2005 Consolidated Balance Sheet. Although the number of material weaknesses was not reduced in fiscal year 2005, many corrective actions were successfully carried out by components. Also, a formal monitoring program was implemented to oversee and measure component progress in carrying out corrective action plans.

- The CFO established an Internal Control Committee to coordinate actions and plan for compliance with the internal control provisions of the Department's Financial Accountability Act. This Act requires the Secretary to include in the *Fiscal Year 2005 Performance and Accountability Report* an assertion on the Department's internal controls over financial reporting. The CFO has already launched plans to meet the Act's fiscal year 2006 audit of internal controls over financial reporting requirement.
- The Department must receive a clean audit opinion on its consolidated financial statements and correct all material weaknesses in internal control before a green score will be possible. To surmount these challenges, the components will need to revamp their corrective action plans, re-

solve all material weaknesses, and more efficiently manage the audit. The internal control audit process, which the Department will undertake in fiscal year 2006, should provide us with the improved tools and insights needed to fully meet the goals of the President's Management Agenda.

EXPANDED ELECTRICAL GOVERNMENT

- The Department worked diligently in fiscal year 2005 to improve the effectiveness and efficiency of the delivery of services, information sharing and enterprise transformation. We achieved this by inventorying the Department's information technology (IT) systems; certifying the security and accreditation of approximately 70 percent of the Department's major IT systems; reviewing 100 percent of all departmental IT exhibits for OMB compliance requirements; increasing earned value monitoring and project management models to ensure that the Department is pursuing the most efficient and cost-effective mission critical systems and investments; and developing the National Information Exchange Model (NIEM) in conjunction with the Department of Justice (DOJ) to standardize Extensible Markup Language (XML) messages to facilitate information sharing within Federal, state, local and tribal governments.
- The Department also increased communication technology through the deployment of the first phase of the Homeland Security Secure Data Network (HSDN) to 56 departmental sites. This network is a unified system and program that enables the sharing and protection of secret-level data between Federal partners.
- The Department used the Homeland Security Enterprise Architecture (HLS EA) Knowledge Repository to reduce duplicative investments, provide the foundation for identification of Transformational Portfolios and ensure optimization of E-Gov implementation. OMB recognized the increased maturity of HLS EA as a tool for information sharing cost reduction with a maturity score of 3.38 up from 2.62 the prior year.
- Finally, the Department improved data accessibility through the creation of the Section 508 Program Management Office (PMO) by the CIO and the Office for Civil Rights and Civil Liberties. The new Section 508 PMO is responsible for ensuring that all electronic and information technologies developed, procured, maintained, or used by the Department are accessible to employees and consumers with disabilities.

IMPROVED BUDGET AND PERFORMANCE INTEGRATION

The Department continued progress in integrating performance-based planning, programming, budgeting and execution. Programming and budgeting is driven to increase performance to achieve the Department's Strategic Plan. The strategic goals and objectives in our plan provided the framework and cornerstone of the *Future Years Homeland Security Program* (FYHSP) and is the road map for driving performance through annual resource planning and program evaluations. We have linked performance goals with resource-allocation plans to form performance-driven budgets. In order to continue a strong linkage between budget and management decisions, strategic planning and program performance, the Department, in the last 12 months, has:

- Developed the fiscal year 2006 to fiscal year 2010 FYHSP - This five-year resource plan, submitted to Congress in March 2005, helps meet strategic goals and objectives by identifying our long-range strategies and resource requirements to implement priority programs. This plan links all programs and associated performance measures and milestones to the Department's strategic goals and objectives. The Department is one of only three departments required by Congress to submit five-year resource and performance requirements.

- Made strategic resource decisions performance based - As part of the programming phase of the Department's process, performance impact of resource alternatives are foremost in operational and investment decisions.
- Linked program goals to program budgets - We linked our fiscal years 2005 and 2006 budget requests to the individual program goals, which collectively achieve the strategic goals and objectives articulated in the Strategic Plan.
- Measured and reported performance on a quarterly basis - The Department established a detailed milestone plan to achieve annual goals and objectives. A performance report is provided to senior managers on a quarterly basis. Progress toward achieving performance goals is reviewed individually and collectively by the Department's managers.

ELIMINATING IMPROPER PAYMENTS

In fiscal year 2005, the Department completed the next phase of its Improper Payments Information Act of 2002 (IPIA) program. This phase focused on establishing baseline estimated improper payment error rates for each component. These rates were obtained by completion of random sample payment testing. Each component tested its program that issued the largest amount of disbursements in fiscal year 2004 (with the exception of EP&R, which tested its second largest program highlighted in an improper payment-related OIG finding). No component was found to have a program at high risk for issuing improper payments (defined by OMB as issuing more than $10 million of improper payments with an error rate above 2.5 percent). Results are listed in Section III, Financial Information.

- Recovery audit contract work at ICE nears completion. To date, $2.2 million of fiscal year 2004 disbursements are improper. This work, which includes components whose accounting services are provided by ICE, has an estimated balance of $1.1 million in remaining improper payments. Recovery audit work at CBP is at an early stage with work expected to fully ramp up next year. Additional components will undergo audit recovery work in fiscal year 2006.
- In fiscal year 2006, the Department anticipates achieving full IPIA compliance by components testing all sizable programs, by expanding recovery audit work, by testing FEMA's Gulf Coast hurricane-related payments, and by completing internal control work.

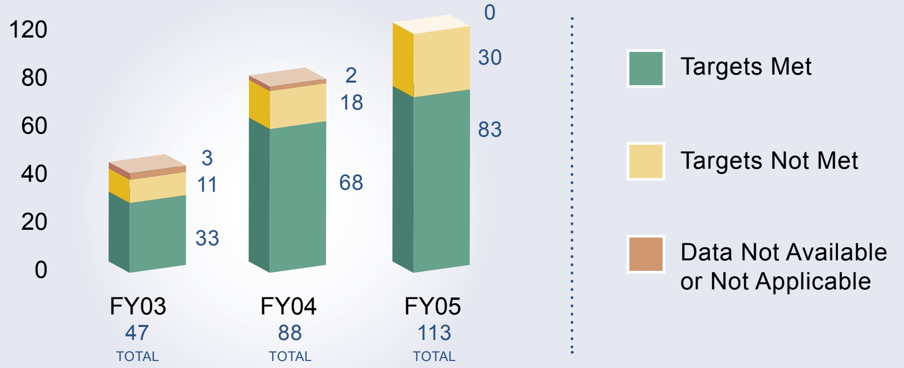
REAL PROPERTY

- Real Property continues to be a challenge for the Department. However, we continue to have an accurate and current inventory in place that is provided to the government-wide real property database. Our next critical steps include finalizing our Asset Management Plan and ensuring that we meet future data reporting requirements.

Performance Highlights

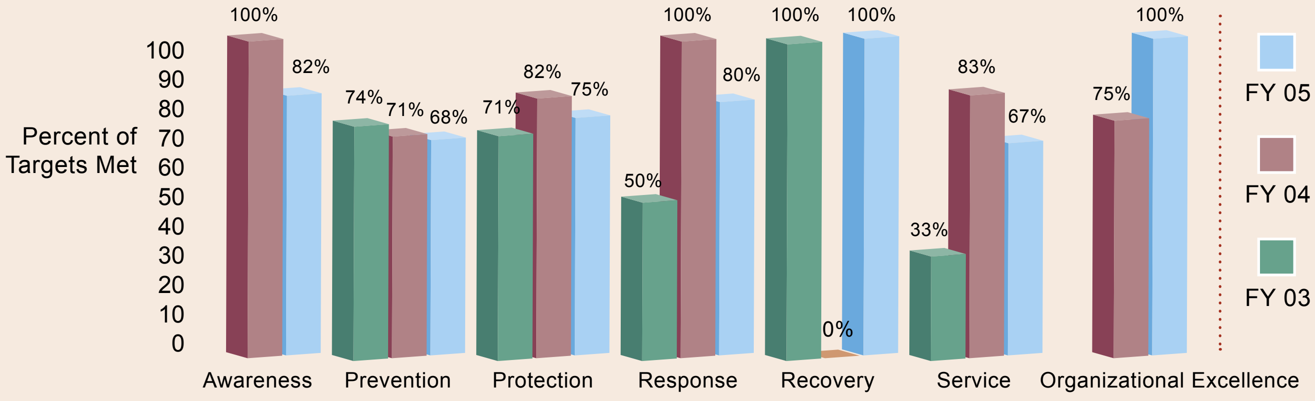
The Department of Homeland Security's seven strategic goals are the framework by which we measure the success of our programs in achieving our mission. We established 113 specific targets under our program goals in fiscal year 2005. Each year we strive to make our targets more aggressive, but this year we met or exceeded 83, or 73 percent, of the established targets. This is a decrease of 4 percent compared to our performance during fiscal year 2004. Reasons for not meeting targets are found in Section II, Performance Information.

DHS PERFORMANCE TRENDS



(When a final target was not available, and an estimate was reported, the target was reported as met or not met in this chart.)

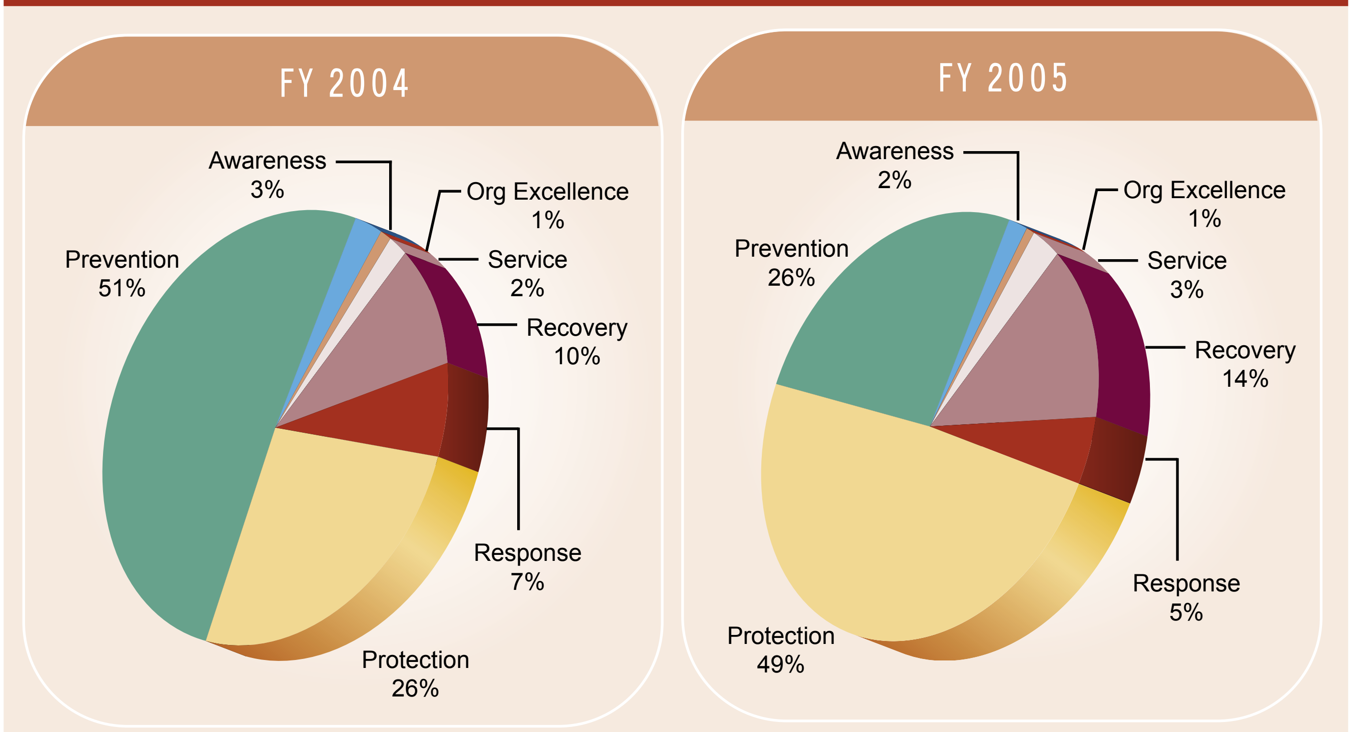
PERFORMANCE TRENDS BY STRATEGIC GOAL



(For fiscal year 2003, there were no targets in the Awareness and Organizational Excellence Strategic Goals)

This section lists the Department's seven strategic goals and the high-level performance measures associated with each, along with an assessment of our performance. We also report our performance and cost information by goal. Detailed information about the Department's performance in fiscal year 2005 is provided in Section II, Performance Information. The net costs of achieving performance in fiscal year 2005 by strategic goal are summarized in the following chart. The gross cost less any offsetting revenue for each Strategic Goal is used to arrive at the net cost shown below.

NET COST BY STRATEGIC GOAL



The total Net Costs equaled $66,405 million in FY 2005.

Strategic Goal 1 ⋆ Awareness

Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.

Objective 1.1	Gather, fuse, and analyze all terrorism and threat related intelligence.
Objective 1.2	Identify and assess the vulnerability of critical infrastructure and key assets.
Objective 1.3	Provide timely, actionable, accurate, and relevant information based on intelligence analysis and vulnerability assessments to homeland security partners, including the public.
Objective 1.4	Develop a Common Operating Picture for domestic situational awareness, including air, land, and sea.

HIGHLIGHTS

In fiscal year 2005, the Department's performance highlights in support of Awareness goals and objectives include the following:

- The IAIP Biosurveillance program improved the Federal government's capability to rapidly identify and characterize a potential bioterrorist attack. The program exceeded its target for the year, 40 percent, by having 50 percent of its recommended National Biosurveillance Integration System (NBIS) process improvement actions accepted and implemented into the NBIS operating procedures. Continual monitoring of program performance and incorporation of lessons learned and best practices was part of the overall NBIS program model.

- IAIP's Critical Infrastructure Identification and Evaluation (CIIE) program exceeded its target of 70 percent by reviewing, researching and cataloging 100 percent of the Critical Infrastructure/Key Resource data call responses into the National Asset Data Base (NADB) within 120 days of receipt. The asset information was submitted by states and territories for more than 48,000 assets.

- The Department enhanced Maritime Domain Awareness in 2005 through USCG's implementation of interagency Joint Harbor Operations Centers (JHOC) and Sector Command Center sensory and intelligence fusion capabilities; improving information sharing through the American Waterway Watch national maritime homeland security program; and starting a counterintelligence service.

- The Department improved information sharing efforts among the national laboratories and the commercial and academic institutions working on Threat Awareness Portfolio (TAP) programs, as well as operational data sharing among Federal, state and local law enforcement agencies through the All-Weapons of Mass Effect assessment, BorderSafe, Enhanced International Travel Security (EITS - international community) and Inter-agency Center for Applied Homeland Security Technology (ICAHST - Interagency collaborations) activities. Installation of pilot TAP technologies at IAIP, CBP and ICE continues providing support to these components' operations.

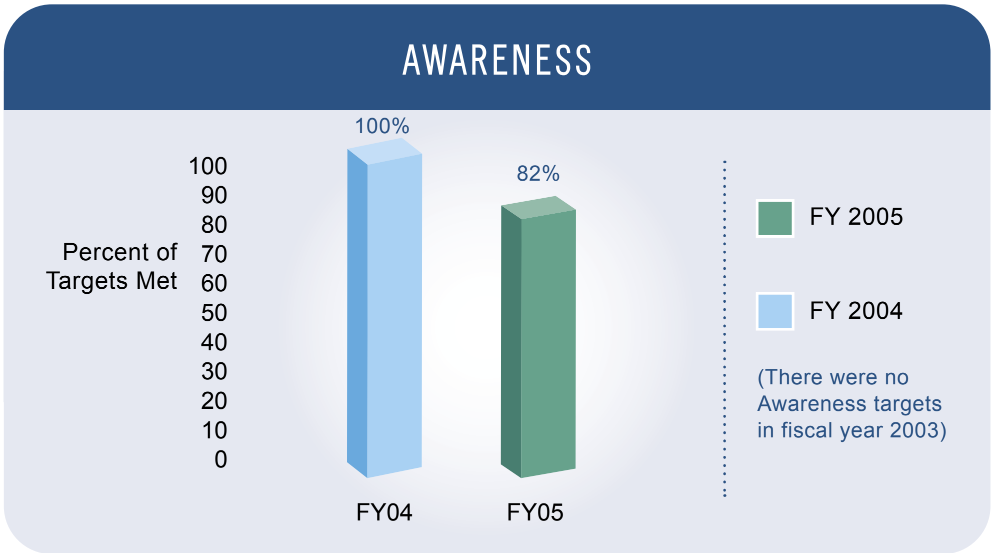
- The Office of Transportation Security Intelligence Services has evaluated the threat to all modes of transportation for which TSA is responsible, prepared baseline assessments for each mode, and packaged these assessments with threat matrices into the "U.S. Transportation Modal Plans Assessments" which is updated as needed. The "U.S. Transportation Modal Plans Assessments" is used in the development of the National Strategy for Transportation Security (NSTS), the Transportation Security Operations Plan (TSOP), and other TSA operational and strategic planning documents.

★ SUCCESS STORY ★

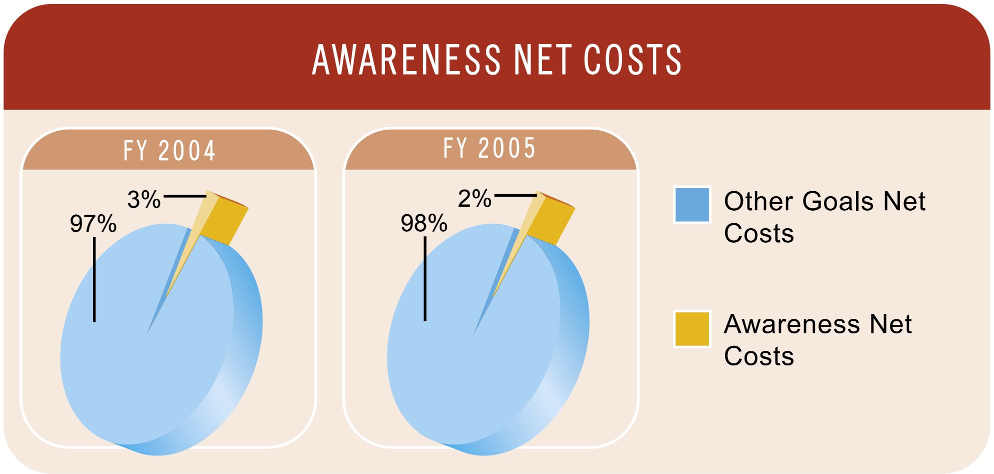
The Department, through the US-VISIT program, enhances public awareness by creating a variety of informational materials. Distributed items include: pamphlets; directional and instructional signage at air, sea and land ports; in-flight videos in 15 languages; a public education campaign in major newspapers in Visa Waiver program countries; a flyer and poster distribution program for visitors in Mexico; public education advertising at the Radio Frequency Identification (RFID) test locations within Mexican and Canadian land borders; and active outreach to global media and stakeholder groups.

Note: You can access additional information at the dhs.gov website.

TRENDS



The Net Costs of this goal in fiscal year 2005 was $1,321 million, or approximately 2 percent of the total Net Costs of the Department's Directorates.



To assess the achievement of all goals, we used quantitative performance measures with targets. These targets were contained in the performance-based budget submitted to Congress. A summary of our fiscal year 2005 performance against those targets is provided in the following scorecard. We report baselines that were successfully established as Target Met in the charts and tables in this section.

PERFORMANCE SCORECARD

Strategic Goal 1 - Awareness

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Infrastructure Vulnerability & Risk Assessment	Improve ability to provide focused information on threats to the U.S. homeland that allows Federal, state, local, tribal and private-sector officials to take meaningful protective action.	100%	◄ ►	157
Evaluations & Studies	Provide National operational communications and information sharing during domestic incidents; collect and fuse information to deter, detect, and prevent terrorist incidents and maintain and share domestic situational awareness.	100%	◄ ►	158
Homeland Security Operations Center	Provide National operational communications and information sharing during domestic incidents; collect and fuse information to deter, detect, and prevent terrorist incidents and maintain and share domestic situational awareness.	0%	▼	158
Threat Determination and Assessment	Support Department of Homeland Security operations and planning functions with timely and actionable intelligence that meets customer requirements.	100%	◄ ►	159

PERFORMANCE SCORECARD

Strategic Goal 1 - Awareness

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Biosurveillance	Function as the lead agency in the development and operation of the National Biosurveillance Integration System (NBIS) to detect biological and chemical attacks and coordinate the real-time integration of biosurveillance data with threat information and recommended responses.	100%	N/A	159
Critical Infrastructure Identification and Evaluation	Identify Critical Infrastructure and Key Resources (CI/KR) and characterize and prioritize these assets based upon the application of appropriate assessment processes and methodologies, using need-specific assessment criteria, sector/segment-specific characterizations, and relevant potential threat information.	100%	N/A	160
Critical Infrastructure Protection	Produce actionable information and recommend reliable technologies to help protect U.S. critical infrastructure.	0%	N/A	161
Domestic Nuclear Detection	Develop an effective suite of countermeasures against radiological and nuclear threats with capabilities in detection and intelligence analysis.	100%	N/A	162
Emerging Threats	Prevent terrorist attacks by developing effective capabilities to characterize, assess, and counter new and emerging threats.	100%	N/A	163
Radiological & Nuclear Countermeasures	Develop an effective suite of countermeasures against radiological and nuclear threats with capabilities in response and preparedness.	100%	N/A	163
Threat and Vulnerability, Testing Assessments	Provide measurable advances in threat discovery and awareness, information management and sharing, linkage of threats with vulnerabilities, and capability and motivation assessments for terrorist organizations required to support Departmental missions to anticipate, detect, deter, and mitigate threats to the United States' homeland security.	100%	N/A	164

* The Performance Goals in the Scorecard are shown as they were stated in the fiscal year 2005 performance plan, but where the goal has been improved, the new goal is shown. Both the old and new goals are shown in the Performance Information tables in Section II of this report. Some goals have been improved to better reflect intended program outcomes.

FUTURE STEPS

Terrorist threats to the nation will not only continue into the future, but also will become increasingly sophisticated. As the nation takes steps to harden potential targets, terrorists will look to exploit other vulnerabilities inherent to an open society. A key to preventing terrorist activity is accurate and timely information.

The Department will continue building an integrated, comprehensive intelligence and warning system to detect terrorist activity before an attack occurs so pre-emptive, preventive and protective actions will be taken. We are putting in place the proper personnel, including a new generation of homeland security analysts, and the facilities and procedures necessary to assemble intelligence collected from a wide variety of homeland security partners. This intelligence will provide a comprehensive view of the most current tactical terrorist threat situation allowing the Department to provide an integrated intelligence package to appropriate recipients, establish threat assessments and conduct long-term strategic terrorism intelligence analysis.

During the next several years, we will focus on developing robust capabilities to assess intelligence collected domestically and abroad and to collect information from a wide variety of sources. That information will be mapped against the nation's vulnerabilities, allowing the Department to issue timely and actionable preventive and protective measures. We will also implement a comprehensive national indications and warning infrastructure with the capacity to provide timely, effective warnings for specific and imminent threats. In addition, the Department will build secure mechanisms and systems for exchanging sensitive homeland security and critical infrastructure information with homeland security officials, using the best features of existing Federal, state, local and private systems. Further, the Department will build an enhanced identification and tracking capability of the maritime approaches and offshore transit routes of the United States.

Strategic Goal 2 ⭑ Prevention

Detect, deter and mitigate threats to our homeland.

Objective 2.1	Secure our borders against terrorists, means of terrorism, illegal drugs and violations of trade and immigration laws.
Objective 2.2	Enforce trade and immigration laws.
Objective 2.3	Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities.
Objective 2.4	Coordinate national and international policy, law enforcement, and other actions to prevent terrorism.
Objective 2.5	Strengthen the security of the Nations transportation systems.
Objective 2.6	Ensure the security and integrity of the immigration system.

HIGHLIGHTS

In fiscal year 2005, the Department's performance highlights in support of Prevention goals and objectives include the following:

- CBP exceeded its goal for the year for the number of border miles under operational control by 92 percent; 288 miles vs. 150 miles. Operational control, as defined in the National Strategic Plan, is the ability to detect, respond to, and interdict border penetrations in areas deemed as high priority for threat potential or other national security objectives.
- CBP improved the targeting, screening, and apprehension of high-risk international cargo and travelers to prevent terrorist attacks, while providing processes to facilitate the flow of safe and legitimate trade and travel. Its Customs-Trade Partnership Against Terrorism (C-TPAT) program enrolls shippers who agree to follow security procedures to secure the supply chain. This results in reduced exams and thereby helps facilitate the flow of trade.
- TSA's Aviation Regulation and Other Enforcement program uses an intensive, risk-based inspection protocol to ensure that airports remain compliant with all applicable laws and regulations. This inspection methodology has ensured that a high level (96.3percent) of all airports nationwide comply with applicable security regulations. By identifying locations that need additional help, TSA provides needed recommendations or sanctions to assist all applicable airports in their goal to reach 100 percent compliance.
- The Department's US-VISIT program's biometric identifiers – specifically digital finger scans and photographs – helped prevent criminals from entering the country by making it virtually impossible for anyone else to claim another's identity should travel documents be stolen or duplicated.

Since the inception of US-VISIT at many of our land, sea and air ports of entry, the use of biometrics has allowed CBP officers at primary inspection locations to deny entry to more than 800 known criminals and visa violators.

- The Department increased operational control of the Southwestern border through CBP's Arizona Border Control initiative. This initiative is a layered approach consisting of placing additional agents on the ground, using specialized teams and rapid-response capabilities, increasing the use of detection technology, improving infrastructure along border areas, and increasing cooperation with local, state and tribal law enforcement entities, as well as with the Mexican government.
- CBP increased enrollment in its global container security program, the Container Security Initiative (CSI). Through CSI, maritime containers that pose a risk for terrorism are identified and examined at foreign ports before they are shipped to the United States. Currently, there are 40 operational CSI ports representing 24 administrations in Europe, Asia, Africa, the Middle East, and North and South America that have committed to the CSI program – including the 20 ports shipping the greatest volume of containers to the United States. Approximately 75 percent of all maritime containers shipped to the United States are being screened through CSI. The goal is to have 50 operational ports by the end of 2006, which will result in approximately 90 percent of all transatlantic and transpacific cargo imported into the United States being subjected to pre-screening.
- CBP fully implemented the Integrated Automated Fingerprint Identification System (IAFIS), now operational in every Border Patrol station throughout the country. This first year of operation resulted in the identification of more than 133,900 individuals with a criminal history attempting an illegal border crossing. Of this group, more than 500 had records of violent crimes.
- A multi-agency task force investigation based in Florida resulted in the seizure of more than five tons of cocaine and the detention of six individuals aboard a fishing vessel in the Eastern Pacific. The size of this seizure is significant for a single vessel and highlights the continuing attempts by organizations to use maritime routes to bring illegal substances to the United States. The task force included the U.S. Attorney for the Middle District of Florida, the USCG, ICE, the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), the Joint Interagency Task Force-South (JIATF-South), the Internal Revenue Service's Criminal Investigative Division, the Florida Department of Law Enforcement, and the Sheriff's Offices of Pinellas and Sarasota counties.
- Members of FLETC's Counterterrorism Division completed the first training courses for Amtrak police. Senior members of Amtrak received the 40-hour Land Transportation Antiterrorism Training Program, sponsored by TSA. These members included the passenger railroad's police, captains, inspectors, and other personnel. Topics included terrorism, bombs and explosives, weapons of mass destruction, special events security, and case studies. The case studies covered suicide attacks, the Madrid bombing, the Chicago cyanide incident, and current events.
- Department of Homeland Security officials on September 29th unveiled the Predator B – Unmanned Aerial Vehicle (UAV) at Ft. Huachuca/Muni-Libby Army Airfield in Arizona. The unmanned aerial system supplements pre-existing intrusion detection and intelligence-gathering devices as well as provides an additional force multiplier within a particular portion of the border. This historic event took place at the home of the largest UAV training facility in the world, where

previous UAV platforms were tested by CBP.

- 90 percent of Federal supervisors rated their FLETC basic training graduate's preparedness as good or excellent. This rate is 17 percent higher than the target for fiscal year 2005, highlighting the quality of instruction at FLETC.

SUCCESS STORY

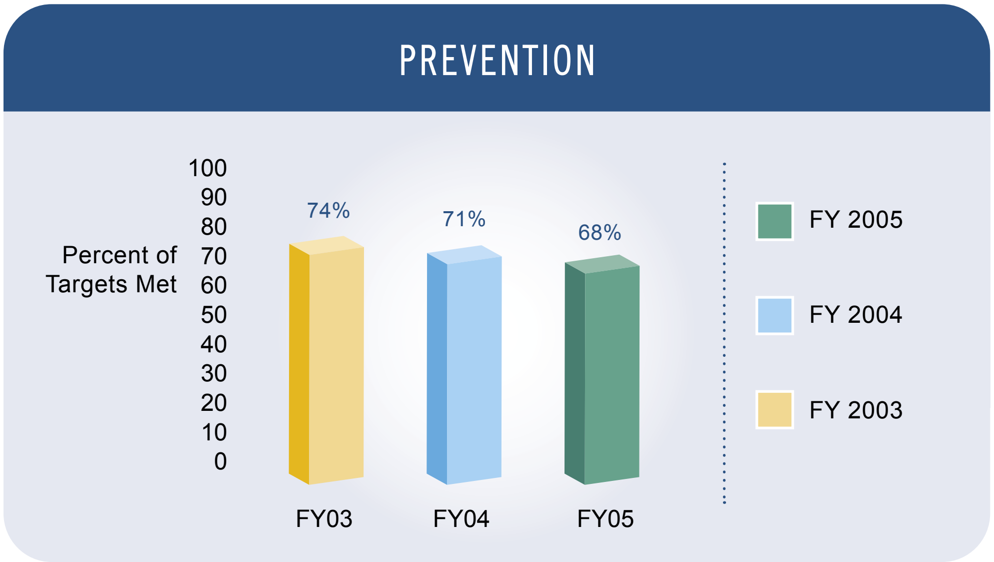
ICE is looking to put money launderers, illegal money services, and others engaged in financial fraud out of business through the use of Suspicious Activity Report (SAR) review teams. ICE agents use the information contained in the SAR to determine if the activity reported rises to a level that warrants further investigation. Disclosure of the subject or existence of a SAR to unauthorized individuals is strictly prohibited. Despite limitations, the SAR continues to be a valuable tool in combating money laundering, terrorist financing, and other serious financial crimes. ICE's SAR reviews identified and led to the successful investigation of the following cases:

- *A California man defrauded a bank of hundreds of thousands of dollars by obtaining stolen checks and depositing them into his own account under a fictitious name. This investigation showed that the man was attempting to further defraud the bank of more than $1 million. The defendant was ordered to make restitution to the bank as part of his sentence. Cntinues on next page*
- *An Atlanta-area business was targeted for investigation by ICE agents for failing to register with the Financial Crimes Enforcement Network (FinCEN) as a money service business. Investigation showed that the owner of this business deposited in excess of $1 million into a bank account, which was subsequently wired abroad to several financial institutions. As a result, agents seized more than $100,000 in currency and property from the violator.*
- *A bank employee was discovered to be involved in Bank Secrecy Act violations based on SAR information filed by a National Capitol Region financial institution. In addition, the funds used as part of the scheme were discovered to have been smuggled from Central America into the United States to avoid currency reporting requirements. The defendant pled guilty to structuring cash deposits and was ordered by the judge to forfeit the currency involved in the scheme.*

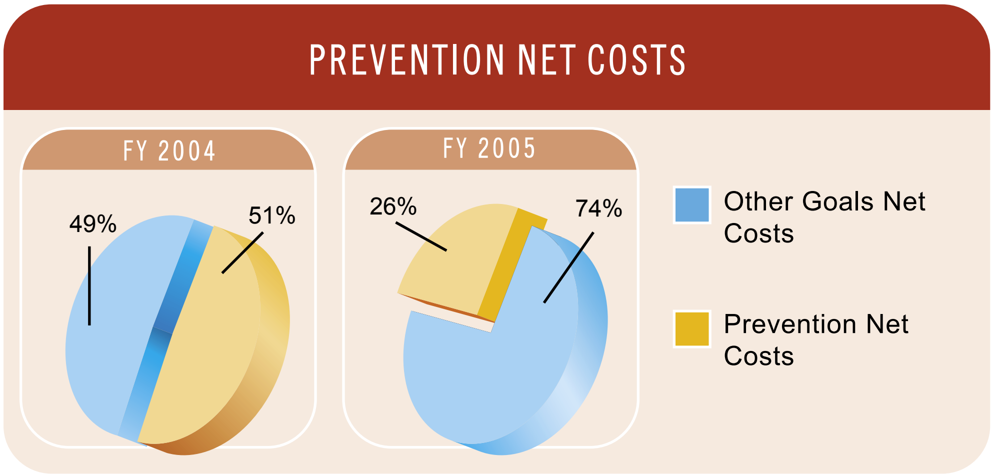
- The total number of recreational boating deaths combined with passenger and maritime worker fatalities and injuries was 1,262. This number is far below our projections for fiscal year 2005. The total number is a combination of the five-year average of passenger and maritime worker fatalities and injuries (572) with the projected annual number of recreational boating deaths (690). This result shows the effectiveness of the USCG's commercial vessel safety and recreational boating safety programs. Of note was the creation of a joint port state control regime for the Great Lakes by the United States and Canada, as well as implementation of the Safety Management System regulatory strategy, which focuses on ensuring that corporate and crew procedures are followed.

- Prior to the September 11th terrorist attacks, the Federal government maintained a list of less than 20 people who were considered a threat to aviation security. Today, that number is over 73,000. TSA has enhanced the Watch List coordination and dissemination process allowing greater sharing of intelligence and law enforcement data. TSA has consolidated watch list operations within the Terrorist Screening Center (TSC) and aligned them with the TSC's Terrorist Screening Database. This effort has greatly increased the quality of the intelligence data contained in the lists and improved the U.S. government's ability to share information regarding personalities who present a threat to national and aviation security.

TRENDS



The Net Costs of this goal in fiscal year 2005 was $17,262 million, or approximately 26 percent of the total Net Costs of the Department's Directorates.



To assess the achievement of all goals, we used quantitative performance measures with targets. These targets were contained in the performance-based budget submitted to Congress. A summary of our fiscal year 2005 performance against those targets is provided in the following scorecard. We report baselines that were successfully established as Target Met in the charts and tables in this section.

PERFORMANCE SCORECARD

Strategic Goal 2 - Prevention

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Office of the Under Secretary, Border and Transportation Security	To maintain the security of our air, land, and sea borders and transportation systems by providing oversight and coordination of Customs and Border Protection, Immigration and Customs Enforcement, the Transportation Security Administration, the Federal Law Enforcement Training Center, the Office of International Enforcement, and the Screening Coordination and Operations Office.	0%	N/A	166
Automation Modernization	Improve the ability of threat, enforcement, travel, and trade information to end users to help ensure lawful, secure, and efficient travel and trade into and out of the United States.	100%	▲	167 - 168
Air & Marine Operations	Deny the use of air, land and coastal waters for conducting acts of terrorism and other illegal activities against the United States.	100%	▲	169
Border Security and Control between Ports of Entry	Prevent potential terrorists, means of terrorism, or other unlawful activities from entering the United States by securing and maintaining control of our borders between the ports of entry.	100%	◀ ▶	169
Border Security Inspections and Trade Facilitation at Ports of Entry	Improve the targeting, screening, and apprehension of high-risk international cargo and travelers to prevent terrorist attacks, while providing processes to facilitate the flow of safe and legitimate trade and travel.	43%	▼	170 - 181
Accreditation	Provide the process based on established law enforcement standards by which law enforcement training programs and facilities are accredited and law enforcement instructors are certified.	50%	◀ ▶	182
Construction and Improvement	Provide law enforcement agents and officers with the knowledge and skills to fulfill their responsibilities in a safe manner and at the highest level of proficiency.	100%	◀ ▶	183
Federal Law Enforcement Training	Provide law enforcement agents and officers with the knowledge and skills to fulfill their responsibilities in a safe manner and at the highest level of proficiency.	100%	◀ ▶	184
International Law Enforcement Training	Provide law enforcement agents and officers with the knowledge and skills to fulfill their responsibilities in a safe manner and at the highest level of proficiency.	100%	◀ ▶	185
State and Local Law Enforcement Training	Provide law enforcement agents and officers with the knowledge and skills to fulfill their responsibilities in a safe manner and at the highest level of proficiency.	100%	◀ ▶	186
Cyber Security	Enable the creation of and migration to a more secure critical information infrastructure.	100%	N/A	187

PERFORMANCE SCORECARD

Strategic Goal 2 - Prevention

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Explosives Countermeasures	Improve explosives countermeasures technologies and procedures to prevent attacks on critical infrastructure, key assets, and the public.	100%	N/A	188
Rapid Prototyping	Identify and rapidly develop, prototype, and commercialize innovative technologies to thwart terrorist attacks.	100%	N/A	188
Standards	Develop well-designed standards and test and evaluation protocols for products, services, and systems used by the Department of Homeland Security and its partners to ensure consistent and verifiable effectiveness. Improve the standardization of products and services designed to prevent and respond to terrorist attacks or natural disasters.	100%	N/A	189
Support to Department of Homeland Security Components	Develop effective technologies and tools to increase the capabilities of the Department of Homeland Security operational components to execute their mission to secure the Homeland.	100%	N/A	190
Air Cargo	Reduce the probability of a successful terrorist or other criminal attack to the air transportation system by improved passenger and baggage screening processes.	100%	◄ ►	191
Compliance and Enforcement	Reduce the probability of a successful terrorist or other criminal attack to the air transportation system by improved passenger and baggage screening processes.	100%	◄ ►	192
Screening Technology	Reduce the probability of a successful terrorist or other criminal attack to the air transportation system by improved passenger and baggage screening processes.	0%	▼	193
Screener Workforce	Reduce the probability of a successful terrorist or other criminal attack to the air transportation system by improved passenger and baggage screening processes.	100%	◄ ►	194
Federal Air Marshal Service	To promote confidence in our nation's civil aviation system through the effective deployment of Federal Air Marshals to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews.	100%	◄ ►	195
Screener Support	Reduce the probability of a successful terrorist or other criminal attack to the air transportation system by improved passenger and baggage screening processes.	100%	◄ ►	196

PERFORMANCE SCORECARD

Strategic Goal 2 - Prevention

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Surface Transportation Security	Reduce effects (psychological, economic, health) of terrorist activities (before, during, after) on surface transportation systems and on the flow of commerce impacted by transportation systems.	100%	◀ ▶	197
Defense Readiness	Support our national security and military strategies by ensuring assets are at the level of readiness required by the combatant commander.	0%	◀ ▶	198
Drug Interdiction	Reduce the flow of illegal drugs entering the U.S. via non-commercial maritime shipping sources.	100%	◀ ▶	199
Marine Safety	Eliminate maritime fatalities and injuries on our Nation's oceans and waterways.	100%	◀ ▶	200
Migrant Interdiction	Eliminate the flow of undocumented migrants via routes to the U.S.	0%	▼	201
Other LE (law enforcement)	Reduce the numbers of vessel incursions into the United States Exclusive Economic Zone (EEZ).	100%	▲	202
Detention and Removal	The Office of Detention and Removal Operations will remove all removable aliens.	0%	▼	203
Office of Investigations	Prevent the exploitation of systemic vulnerabilities in trade and immigration that allow foreign terrorists, other criminals, and their organizations to endanger the American people, property, and infrastructure.	100%	▲	204

* The Performance Goals in the Scorecard are shown as they were stated in the fiscal year 2005 performance plan, but where the goal has been improved, the new goal is shown. Both the old and new goals are shown in the Performance Information tables in Section II of this report. Some goals have been improved to better reflect intended program outcomes.

FUTURE STEPS

The Department's main priority is to prevent further terrorist attacks against the nation. By managing who and what enters the United States, we will work to prevent the entry of terrorists and instruments of terror while facilitating the legitimate flow of people, goods and services. During the next five years, the Department will continue to create coherent screening, targeting and risk-management approaches across activities, including the capacity for transmitting and receiving advanced information about people and commercial shipments approaching the United States. We will enhance real-time monitoring and surveillance of the border, including seaports, landports, airports, and between ports of entry. The Department will build an integrated system that detects, identifies and tracks high-threat vehicles in the air, land and maritime domains, and share this information with appropriate stakeholders. We will implement a program to identify, track and intercept chemical, biological, radiological, nuclear and explosive components and systems at ports of entry and, where practicable, in intermodal transportation systems within U.S. borders. Additionally, the Department will project apprehension rates and ensure that detention space is available to support our detention and removal efforts.

Strategic Goal 3 ⋆ Protection

Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters or other emergencies.

Objective 3.1	Protect the public from acts of terrorism and other illegal activities.
Objective 3.2	Reduce infrastructure vulnerability from acts of terrorism.
Objective 3.3	Protect our Nations financial infrastructure against crimes, to include currency and financial payment systems.
Objective 3.4	Secure the physical safety of the President, Vice President, visiting world leaders and other protectees.
Objective 3.5	Ensure the continuity of government operations and essential functions in the event of crisis or disaster.
Objective 3.6	Protect the marine environment and living marine resources.
Objective 3.7	Strengthen nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies.

HIGHLIGHTS

In fiscal year 2005, the Department's performance highlights in support of Protection goals and objectives include the following:

- SLGCP's State Preparedness Grants program increased the capability of states and territories to prevent, protect, respond, and recover from all-hazard events. The 40 percent of jurisdictions demonstrating acceptable performance on applicable critical tasks in exercises using State SLGCP approved scenarios exceeded the target of 23 percent. This improvement in jurisdictions' performance on critical tasks over time reflects the impact of SLGCP preparedness activities (including activities supported by the State Preparedness Grants Program) on jurisdictions' overall preparedness levels.
- 487,414 state and local homeland security preparedness professionals were trained in fiscal year 2005, 39 percent above the SLGCP State and Local Training Program target for the year. This demonstrates the significant breadth of the State and Local Training Program in training hundreds of thousands of homeland security professionals to improve their capabilities, thus increasing the nation's overall preparedness.
- Campaign 2004 protective activities concluded in November 2004. Throughout the campaign, the Secret Service provided security advances to presidential candidates and their immediate families.

- The 2005 Presidential Inauguration was a National Special Security Event (NSSE) held in Washington, D.C., on January 20, 2005. The Inaugural security plan involved the coordination of 15 Federal agencies and 22 state and local police and emergency service resources, including the Washington, D.C., Metropolitan Police Department. The Department's TSA, FEMA, IAIP and National Capital Region also assisted the Secret Service. The Secret Service used a variety of non-traditional and traditional security measures, including counter surveillance of venues, controlled access to the parade route and event sites, and magnetometer screening of more than 297,000 people attending these events.

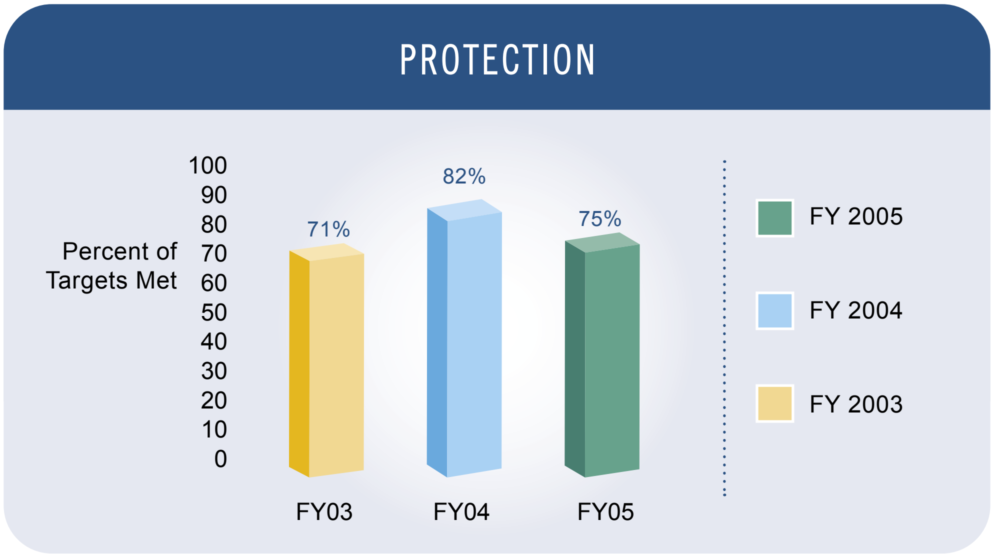
SUCCESS STORY

The Secret Service expanded its Electronic Crimes Special Agent Program (ECSAP), which allows agents to respond to the ever-increasing scope of electronic crimes investigations. It also developed a system to provide financial partners with a report-based strategic analysis of financial fraud data as provided by multiple industry partners. These developments contributed to protecting the public against electronic and financial crimes by preventing $556 million in losses.

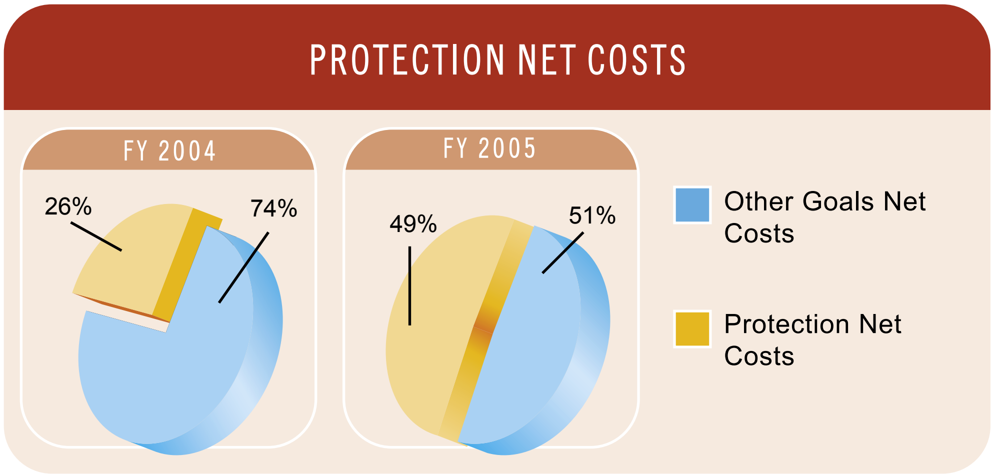
- As part of the Presidential election threat disruption effort, ICE agents completed more than 900 intelligence-based investigations, and made 237 arrests, between October and November 2004, targeting immigration status violators in the United States who posed potential national security risks or criminal threats.
- ICE arrested 21 fugitive aliens following an 11-day operation that targeted criminal aliens in Wisconsin who were hiding to avoid deportation orders issued by Federal judges. 6 of those arrested were felons with prior convictions that range from drug dealing to bank fraud, battery, and robbery. An additional 4 had criminal histories ranging from assault to criminal damage of property.
- The "No Safe Haven" initiative made great strides at bringing human rights abusers to justice in the United States. In fiscal year 2005, ICE arrested 16 human rights violators, and 135 criminal investigations are pending. This initiative seeks to deny refuge in the United States to international human rights violators by identifying, investigating, prosecuting and removing them from the country and by preventing violators from entering the country.
- The USCG met its goal of lowering maritime security risk. This outcome resulted from: complete verification of security plans for U.S. port facilities and vessels operating in U.S. waters, achievement of "interim operating capability" for 5 new maritime safety and security teams, completion of 31 foreign port security assessments, and development of explosive detection and anti-small vessel capabilities.
- Completed the third full-scale exercise in the Department's Top Officials series, known as TOPOFF 3, which was the largest and most comprehensive terrorism-response exercise ever conducted, involving more than 10,000 participants from more than 275 government and private-sector organizations. It was also the first time a European country was involved. The drills, which ran from April 4 to 8, allowed first responders in New Jersey, Connecticut, Canada and

the United Kingdom to test how prepared they are to face terrorist attacks involving weapons of mass destruction. TOPOFF 3 was the first simulation to follow the new National Response Plan and use National Incident Management System protocols. The exercise was carefully analyzed to obtain lessons learned.

TRENDS



The Net Costs of this goal in fiscal year 2005 was $32,459 million, or approximately 49 percent of the total Net Costs of the Department's Directorates.



To assess the achievement of all goals, we used quantitative performance measures with targets. These targets were contained in the performance-based budget submitted to Congress. A summary of our fiscal year 2005 performance against those targets is provided in the following scorecard. We report baselines that were successfully established as Target Met in the charts and tables in this section.

PERFORMANCE SCORECARD

Strategic Goal 3 - Protection

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Mitigation	Reduce the impact of natural hazards on people and property through the analysis and reduction of risks and the provision of flood insurance.	0%	▼	206
National Security	All Federal departments and agencies will have fully operational Continuity of Operations (COOP) and Continuity of Government (COG) capabilities.	0%	◀ ▶	207
Preparedness	Assess Federal and State implementation of the National Incident Management System (NIMS), train the Nation's Disaster and emergency personnel, and reduce loss of life from fire in the United States.	0%	◀ ▶	208
Critical Infrastructure Outreach & Partnerships	Build strategic partnerships between Department of Homeland Security (DHS)/Information Analysis Infrastructure Protection (IAIP) and critical infrastructure owners & and operators to support two-way information sharing.	100%	N/A	209
Cyber Security	Prevent, detect, and respond to Cyber Security Events.	100%	N/A	210
Evaluation and National Assessment Program	Improve our process and procedures by implementing recommendations of reviewing authorities (i.e. IG, OMB, GAO).	100%	◀ ▶	211
Fire Act Program	The health and safety of the public and firefighting personnel against fire and fire-related hazards are minimized by providing direct assistance, on a competitive basis, to fire departments of a state or tribal nation.	67%	▼	212 - 214
National Exercise Program	Improve the capability of the Nation's first responders to prevent, respond to, and recover from acts of terrorism by periodically exercising together, thereby enhancing the Nation's preparedness.	50%	◀ ▶	215 - 216
National Infrastructure Simulation and Analysis Center	Provide comprehensive infrastructure-related modeling, simulation and analytic capabilities to support protective action planning and implementation decision processes.	100%	NA	217
National Security/Emergency Preparedness Telecommunications	By fiscal year 2011 reach 95% for Government Emergency Telecommunications Service (GETS) call completion rate during periods of network congestion.	100%	◀ ▶	218

PERFORMANCE SCORECARD

Strategic Goal 3 - Protection

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Protective Actions	Build sustainable protective capacity by developing and facilitating the implementation of protection strategies, security best practices and protective programs that reduce the risk from current and emerging threats, based on sector/segment-specific vulnerabilities of Critical Infrastructure/Key Resources (CI/KR).	100%	N/A	219
State Preparedness Grants Program	Enhance the capability of states and territories to prevent, protect, respond and recover from all-hazard events through the provision of grants.	50%	◀ ▶	220 - 221
State and Local Training	Improve the ability of first responders to prevent, protect against, respond to, and recover from acts of weapons of mass destruction (WMD) terrorism and other disasters by administering a comprehensive training program tailored to responder communities.	100%	◀ ▶	222 - 223
Urban Areas Security Initiative	Through the award of grant funds, improve the protection of our Nation's critical transportation systems, high-risk urban areas, and critical infrastructure from terrorism, especially explosives and non-conventional threats, that would cause major disruption to commerce and significant loss of life.	50%	◀ ▶	224 - 225
Technical Assistance	Enhance state and local jurisdiction preparedness strategies related to chemical, biological, radiological, nuclear, and explosives (CBRNE) terrorism, as well as other hazards such as hurricanes and floods, through the provision of information resources, stand-alone tools, and customized on-site assistance.	100%	◀ ▶	226
Biological Countermeasures	Provide dependable risk analyses, effective systems for surveillance and detection, and reliable bioforensic analysis to protect the Nation against biological attacks.	100%	N/A	227
Counter Man-Portable Air Defense System	Provide effective and economical capabilities to dramatically reduce the threat to commercial aircraft posed by man-portable anti-aircraft missiles.	100%	N/A	228
SAFETY Act	Encourage the development and deployment of anti-terrorism technologies by awarding SAFETY Act benefits to homeland security technology producers.	100%	N/A	229
University Programs	Engage a broad network of universities to provide high quality research to develop the science and intellectual capacity needed to support the Department of Homeland Security's mission of confronting terrorism and responding to natural disasters and educational programs to increase the number of U.S. students in academic fields related to homeland security.	100%	N/A	230

PERFORMANCE SCORECARD

Strategic Goal 3 - Protection

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Living Marine Resources	Achieve sustained fisheries regulation compliance on our nation's Oceans.	0%	◄ ►	231
Ports Waterways and Coastal Security	Reduce homeland security risk in the maritime domain.	100%	▲	232
Protection of Federal Assets-Federal Protective Service	Provide law enforcement, criminal investigations, and physical security protection to reduce and respond to potential threats and vulnerabilities to Federal properties thereby providing a safe, secure environment to Federal tenants and the visiting public in a cost-effective manner.	100%	◄ ►	233
Campaign Protection	Protect our presidential and vice presidential candidates and nominees.	100%	◄ ►	234
Domestic Protectees	Protect the Nation's leaders and other protectees.	100%	◄ ►	234
Financial Investigations	Reduce losses to the public attributable to counterfeit currency, other financial crimes, and identity theft crimes that are under the jurisdiction of the Secret Service, which threaten the integrity of our currency and the reliability of financial payment systems worldwide.	50%	▼	235
Foreign Protectees and Foreign Missions	Protect visiting world leaders.	100%	◄ ►	236
Infrastructure Investigations	Reduce losses to the public attributable to electronic crimes and crimes under the jurisdiction of the Secret Service that threaten the integrity and reliability of the critical infrastructure of the country.	100%	◄ ►	236
Protective Intelligence	Reduce threats posed by global terrorists and other adversaries.	100%	◄ ►	237

* The Performance Goals in the Scorecard are shown as they were stated in the fiscal year 2005 performance plan, but where the goal has been improved, the new goal is shown. Both the old and new goals are shown in the Performance Information tables in Section II of this report. Some goals have been improved to better reflect intended program outcomes.

FUTURE STEPS

The Department is leading a systemic, comprehensive and strategic effort to reduce the country's vulnerability to terrorist attack. We, along with other agencies, are working to identify, prioritize and coordinate the protection of critical infrastructure and key resources to prevent and mitigate the effects of deliberate efforts to destroy, incapacitate or exploit these assets. Specific emphasis is placed on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties. The Department is strengthening Federal law enforcement communities, augmenting the scope and quality of information available to them, and providing tools to assist them in stopping those who wish to do this country harm.

During the next five years, the Department will continue to integrate law enforcement functions to maximize effectiveness and minimize duplication. We will create a rigorous document fraud detection and development system that produces documents of high integrity, while thwarting forgeries and fabrications. The Department will also enhance and maintain a nationwide critical infrastructure and key-asset registry with geospatial data that focuses on identifying and prioritizing infrastructure and key resources. We will develop the capacity to "map" intelligence threat information to vulnerability assessments and choreograph an interactive relationship between analysis of threats against the Homeland, comprehensive vulnerability assessments and domestic preventative and protective measures. The Department will establish a baseline understanding of and continuing capacity to monitor the "health" of cyber and physical infrastructure as a foundation for indications and warning efforts. We will develop the capability to provide early warning about cyber attacks, vulnerability disclosure and emergency response. We will provide state, local and private sectors with information, training and services to implement measures to effectively and consistently protect infrastructure. Additionally, the Department will implement a national continuance of government and operations program that will allow every department to continue, should an emergency occur, including off-site data storage and analysis redundancies.

The Department's work in improving our ability to detect and prevent chemical, biological, radiological and nuclear threats to the nation will reduce our vulnerability. We are establishing national priorities in the development of technologies to recognize, identify and confirm the occurrence of a terrorist attack and thereby minimize casualties. The Department will strengthen the nation's preparedness by focusing Federal, state and local efforts on a cohesive, mutually reinforcing response capability. We will develop an attack warning and characterization system that provides early warning and detection of biological attacks and assists in guiding response actions. We will also create a nationwide exercise program to maintain high preparedness standards for jurisdictions. Finally, the Department will implement a nationwide training program for first responders that will include basic chemical, biological, radiological and nuclear response capabilities.

Strategic Goal 4 ⭑ Response

Lead, manage and coordinate the national response to acts of terrorism, natural disasters or other emergencies.

Objective 4.1 Reduce the loss of life and property by strengthening response readiness.
Objective 4.2 Provide scalable and robust all-hazard response capability.
Objective 4.3 Provide search and rescue services to people and property in distress.

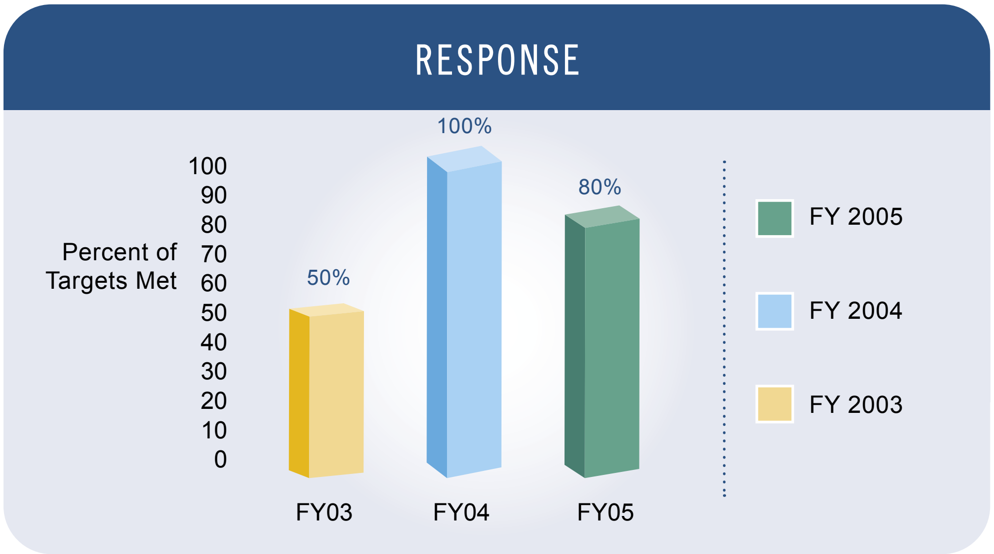
HIGHLIGHTS

In fiscal year 2005, the Department's performance highlights in support of Response goals and objectives include the following:

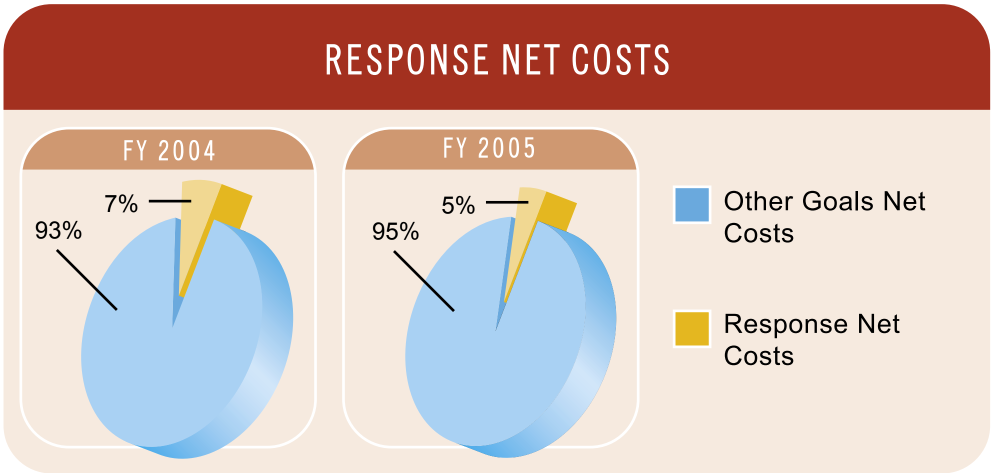
- S&T's Chemical Countermeasures program met its target to develop a prototype mobile laboratory capable of on-site, high throughput analysis of Toxic Industrial Chemicals (TIC) and Chemical Warfare Agents (CWA). Additionally, the program initiated an evaluation of the risks, vulnerabilities, and consequences due to attacks using the TIC cyanide.
- Hurricane Katrina was one of the largest search-and-rescue operations in U.S. history. The USCG used air and boat crews to rescue more than 24,100 people and assisted with the joint-agency evacuation of an additional 9,400 patients and medical personnel from hospitals in the Gulf Coast region. More than 33,500 lives have been saved and evacuated to date:
  - 12,535 lives saved by air resources.
  - 11,600 lives saved by surface resources.
  - 9,409 patients evacuated from hospitals.

  In addition, the USCG saved 138 lives before and after Hurricane Rita.
- In response to Hurricane Katrina, more than 600 TSA employees were flown to Louis Armstrong New Orleans International Airport to help evacuate 23,500 people, many of whom were ill.
- At the close of fiscal year 2005, the USCG met its aggressive goal of limiting the five year-average number of spills to 18.4 per one hundred million short tons shipped. Key to attaining this performance was the USCG's use of the National Interagency Incident Command System (ICS) model in the United States' National Response Plan. ICS provides a unified framework to tie together the efforts of maritime industries, and local, state and Federal officials in responding to catastrophic environmental threats.

TRENDS

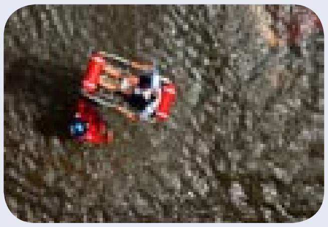

RESPONSE

The Net Costs of this goal in fiscal year 2005 was $3,453 million, or approximately 5 percent of the total Net Costs of the Department's Directorates.


RESPONSE NET COSTS

SUCCESS STORY

LOUISIANA - Coast Guard Petty Officer 2nd Class Scott D. Rady of Airstation Clearwater, Florida, gives the signal to hoist an expectant mother from her apartment building following Hurricane Katrina. In all, the Coast Guard rescued 24,135 victims from this particular storm, including more than 12,000 survivors by helicopter.



To assess the achievement of all goals, we used quantitative performance measures with targets. These targets were contained in the performance-based budget submitted to Congress. A summary of our fiscal year 2005 performance against those targets is provided in the following scorecard. We report baselines that were successfully established as Target Met in the charts and tables in this section.

PERFORMANCE SCORECARD

Strategic Goal 4 - Response

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Response	Consistently achieve fully operational status for all multi-disciplinary response teams, and meet established average response times.	100%	◄ ►	239
Chemical Countermeasures	Provide dependable risk analyses, effective systems for surveillance, detection, and restoration, and reliable laboratory analytical analyses to protect the Nation against attacks involving chemical agents.	100%	N/A	240
Interoperability & Compatibility	Ensure interoperability and compatibility between emergency response agencies at the local, state and Federal levels and standardize Federal testing and evaluation efforts for emergency response technologies.	0%	N/A	241
Marine Environmental Protection	Eliminate oil spills and chemical discharge incidents.	100%	◄ ►	242
Search and Rescue	Save mariners in imminent danger on our Nation's oceans and waterways.	0%	▼	243

* The Performance Goals in the Scorecard are shown as they were stated in the fiscal year 2005 performance plan, but where the goal has been improved, the new goal is shown. Both the old and new goals are shown in the Performance Information tables in Section II of this report. Some goals have been improved to better reflect intended program outcomes.

FUTURE STEPS

In the span of one month, nature dealt two very significant blows to the Gulf Coast. As a result of Hurricanes Katrina and Rita, many have lost loved ones and millions have seen their lives uprooted and their livelihoods destroyed.

In particular, Hurricane Katrina will go down as one of the worst natural disasters in our nation's history. As a result of this storm, more than 1.5 million people evacuated the Gulf Coast, nearly 250,000 homes have been damaged or destroyed, and over 1,200 lives have been lost. An estimated 600,000 people have required sheltering, compared to 180,000 people for the four hurricanes that struck Florida in 2004.

While the federal response to Hurricane Katrina was unprecedented, it was certainly not without flaws. The shared goal must be to replicate the things that went well – and to eliminate the things that did not. This tragedy has emphasized how critical it is that planning and response capabilities perform with seamless integrity and efficiency in any type of disaster situation – even one of cataclysmic nature. Furthermore, it emphasized the importance of having accurate, timely and reliable information about true conditions on the ground, the lack of which frustrated the best efforts to coordinate the response with federal, state and local officials.

With Hurricane Rita, the federal response effort functioned much more efficiently – admittedly in a less extreme environment. Just two weeks out from Hurricane Katrina, improvements in communication and coordination between levels of government were already evident. But that is only one step in ensuring the Department identifies the lessons learned from Hurricane Katrina and makes the necessary adjustments.

Some of the very first images on television after Hurricane Katrina were of USCG helicopters rescuing stranded citizens on rooftops and in rising floodwaters. These brave men and women performed selfless acts of courage, contending with high winds, flying debris and downed power lines. In all, the USCG rescued more than 33,500 people in its response to Hurricane Katrina – six times the number of people it rescued in all of 2004. At its peak, USCG assets supporting the Hurricane Katrina response totaled 65 aircraft, approximately 30 cutters, approximately 100 boats, and nearly 5,000 personnel.

In addition, TSA helped organize "Operation Air Care," the largest domestic civilian airlift ever in our nation's history. More than 23,000 stranded evacuees were lifted to safety from the New Orleans Airport. These efforts were also supported by the Federal Air Marshal Service, the Department of Transportation, the Air Transport Association, and some of our nation's largest air carriers.

By October, FEMA had provided almost $2.9 billion in vital disaster aid to more than 1.6 million affected households. That is in addition to millions of dollars in generous donations from other organizations and the American people.

CBP and ICE also provided a combined 1,300 law enforcement officers to New Orleans to help maintain order and protect critical assets until additional National Guard troops could be mobilized. And the Secret Service provided strategic aid and support at critical locations, including the Superdome in New Orleans and the Astrodome in Houston.

But there are many things that did not work well with the response. As the Department completes after action reviews, more comprehensive improvements in catastrophic preparedness and response capabilities will be made.

Through this review process, the Department will continue to gather facts and information, but the reality is the Department will not wait for the review's completion to adapt and improve.

There are three areas the Department must address immediately to begin the process of strengthening the system. These are:

- Improve FEMA's overall capacity to enhance this vital agency's capabilities so that it can fulfill its historic and critical mission supporting response and recovery.
- Enhance communications and information sharing capabilities. In any disaster, situational awareness requires real time access to accurate, first-hand information.
- Fundamentally strengthen and elevate the role of preparedness to ensure that preparedness efforts have focused direction.

Improving the nation's ability to respond to disasters, man-made or natural, is a top priority for the Department. The Department is improving its capabilities and preparing those who respond to acts of terror and other emergencies. Our priority is ensuring connectivity and interoperability with the appropriate Federal, state and local entities that are accountable for response.

During the next five years, the Department will continue strengthening a National Incident Management System (NIMS) to develop incident management expertise, interoperable standards for incident response, and maintain and provide a forum for increased dialog and cross training among response communities. We will also develop a single, comprehensive and seamless incident command apparatus using the capabilities, assets and expenditures of all departmental entities. The Department will implement an interoperable, safe and reliable communications system to ensure an effective response to crisis. Additionally, we will build a comprehensive package of strategically pre-positioned response equipment, available trained personnel, supplies and transportation assets.

We will strengthen the nation's ability to respond to emergencies by integrating departmental response systems and teams and completing catastrophic all-hazard plans for the most vulnerable communities. The Department will provide health and medical response readiness through integrated planning, surge capacity capabilities and availability of vaccines and medical supplies to address health and medical emergencies or acts of terrorism. We will deliver emergency housing to large displaced populations following major disasters. We will provide a Federal medical response capability that supplements state and local disaster response by: enhancing National Disaster Medical System team readiness and capability, reducing the average team response time, and increasing the percentage of fully operational Disaster Medical Assistance teams. The Department will coordinate an effective response when state, local and tribal resources are overwhelmed.

Strategic Goal 5 ★ Recovery

Lead national, state, local and private-sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters or other emergencies.

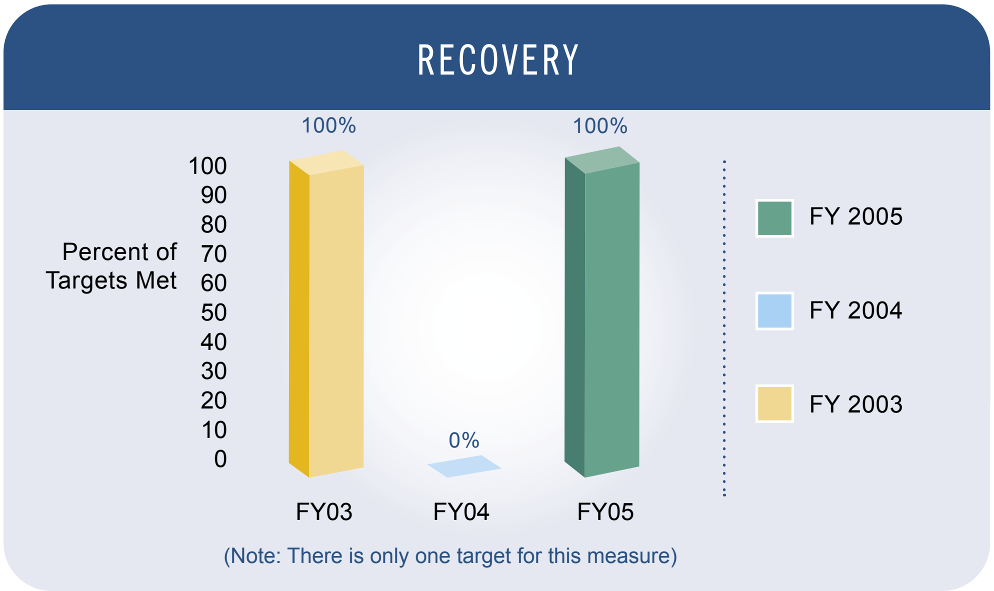
Objective 5.1 Strengthen nationwide recovery plans and capabilities.
Objective 5.2 Provide scalable and robust all-hazard recovery assistance.

HIGHLIGHTS

In fiscal year 2005, the Department's performance highlights in support of Recovery goals and objectives include the following:

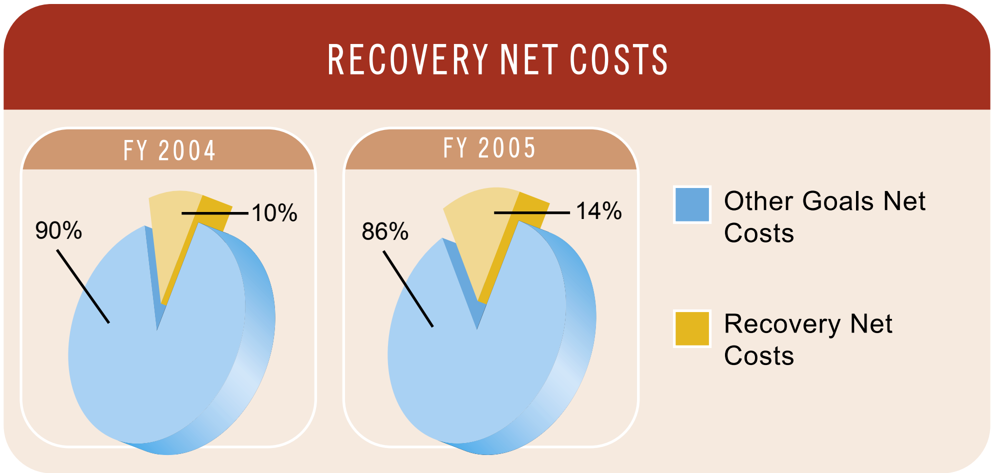
- More than 4,000 USCG, 12,000 FEMA, and 2,500 Federal law enforcement personnel were deployed to support Hurricanes Katrina and Rita relief operations.
- IAIP's National Communications System (NCS) office supervised and coordinated telecommunications restoration and recovery efforts between government and industry during Hurricanes Katrina and Rita. NCS distributed 115,000 Government Emergency Telecommunications Service (GETS) cards. More than 32,000 GETS calls were made in support of Hurricane Katrina with a 95 percent success rate.
- In the area affected by Hurricanes Katrina and Rita, 1,169 maritime aids to navigation had discrepancies reported. Damage was primarily to beacons and buoys, which provide navigation information invaluable to determining location, dangerous areas, and directions of travel on the water. By year end, 850 aids to navigation were reset or repaired.
- The USCG has closed 699 of 1,159 pollution cases stemming from Hurricanes Katrina and Rita.
- FEMA, in conjunction with other Federal agencies, helped recovery efforts after hurricanes Katrina and Rita. Federal support to state and local officials, volunteer organizations and families devastated by Hurricane Katrina continues around the clock. Federal benefits as of the end of the fiscal year include:
  - Katrina total expedited financial assistance awarded: $2.4 billion to 688,000 households.
  - Rita total expedited financial assistance amount awarded: $78 million to 37,000 households.
  - Total Transitional Housing Assistance awarded: $748 million reflecting 317,000 approved applications.

TRENDS



(Note: There is only one target for this measure)

The Net Costs of this goal in fiscal year 2005 was $9,451 million, or approximately 14 percent of the total Net Costs of the Department's Directorates.



To assess the achievement of all goals, we used quantitative performance measures with targets. These targets were contained in the performance-based budget submitted to Congress. A summary of our fiscal year 2005 performance against those targets is provided in the following scorecard. We report baselines that were successfully established as Target Met in the charts and tables in this section.

PERFORMACE SCORECARD

Strategic Goal 5 - Recovery

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Recovery	Ensure disaster recovery capability that restores services to individuals and rebuilds communities in non-catastrophic disasters with a high degree of customer satisfaction, while reducing cost and assistance cycle times and providing for recovery from catastrophic disasters.	100%	▲	245

* The Performance Goal in the Scorecard is a new goal. Both the old and new goals are shown in the Performance Information tables in Section II of this report. Some goals have been improved to better reflect intended program outcomes.

FUTURE STEPS

The Department leads the nation in coordinating recovery from disasters. In the event of a national emergency, the Department is prepared to lead Federal, state, local and private-sector efforts to help rebuild communities and restore services. We will lead long-term recovery including assessing losses, identifying infrastructure recovery actions and rebuilding the capabilities of local partners.

For the hundreds of thousands of families who have lost their homes and their communities as a result of Hurricane Katrina, the Department, working with other federal agencies, will take action to ease the burdens and the challenges of their ordeal.

The government has a duty to these survivors and must help care for those who have lost everything – and help restore their hope and their control of their lives. As President Bush made clear, “we will do what it takes, we will stay as long as it takes, to help citizens rebuild their communities and their lives.”

FEMA is not itself a first responder – but it does play a critical role in working with state and local first responders in their response and recovery efforts. State and local authorities not only possess the intimate knowledge and understanding of their home communities and their response capabilities, but they have both the legal authority and constitutional responsibility to protect and provide for their own citizens. FEMA also plays an essential role in providing additional support in the weeks and months following an incident, such as individual disaster assistance and temporary housing.

FEMA worked hard to move evacuees from temporary shelters into transitional housing. The number of people living in shelters declined from more than 273,000 to less than 12,000 by October– a decrease of more than 95 percent – despite additions resulting from Hurricane Rita.

FEMA must be better prepared to deal with all stages of a truly catastrophic event like Hurricane Katrina. For the vast majority of natural disasters, FEMA’s current capabilities are sufficient to handle the needs of affected populations. This was demonstrated in 2004 when FEMA responded to a record 68 major disasters, including 27 hurricane-related disasters in 15 states.

But with Hurricane Katrina, these capabilities were pushed beyond the breaking point. FEMA must be prepared to anticipate both short-term and long-term needs of impacted communities. That includes having housing plans already in place for feeding and sheltering in excess of 500,000 evacuees, improving our system for rapid distribution of emergency funds, working with federal partners to develop effective anti-fraud measures, and having debris removal plans in place so that supplies are not held up because of impassible roads and so communities can more quickly begin rebuilding and repopulating impacted areas. State and local governments will need to have full awareness of how these capabilities link up with their efforts.

In all of these areas, FEMA must be strengthened not just for its own sake but so that the Federal Government is more effective at helping state and local partners better respond to and recover from catastrophic events.

★ SUCCESS STORY ★

LOUISIANA - Petty Officer 3rd Class Jason Spence of Coast Guard Sector New Orleans and Petty Officer 1st Class Marc San Filippo of the Coast Guard Pacific Strike Team assess an oil spill at the Bass Oil Facility south of New Orleans. The two storage tanks failed during the height of Hurricane Katrina when an estimated 3.8 million gallons of crude oil were released into the tank berm and surrounding marsh lands. Although efforts are ongoing, the Coast Guard has already successfully recovered an estimated 1.1 million gallons of oil from this spill.

Strategic Goal 6 ⋆ Service

Serve the public effectively by facilitating lawful trade, travel and immigration.

Objective 6.1	Increase understanding of naturalization, and its privileges and responsibilities.
Objective 6.2	Provide efficient and responsive immigration services that respect the dignity and value of individuals.
Objective 6.3	Support the United States humanitarian commitment with flexible and sound immigration and refugee programs.
Objective 6.4	Facilitate the efficient movement of legitimate cargo and people.

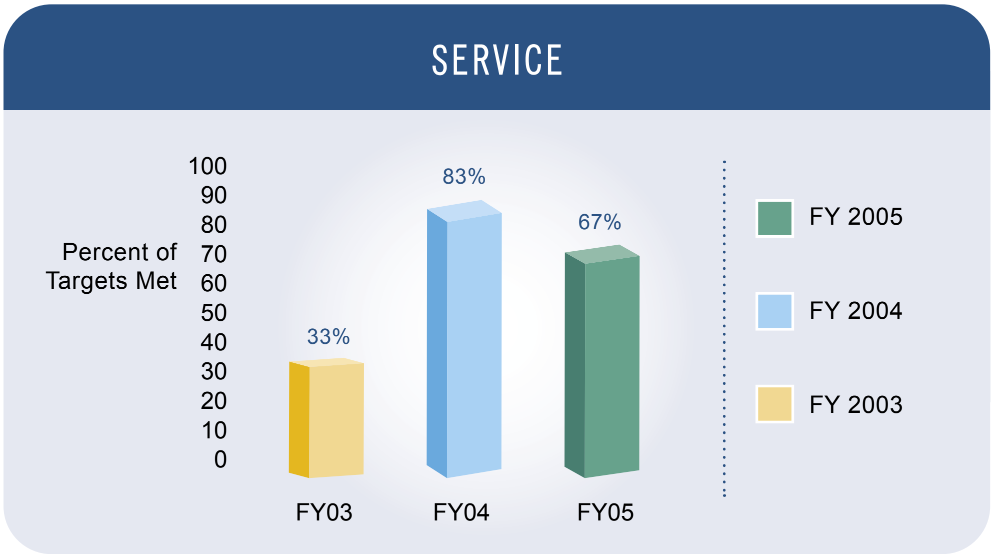
HIGHLIGHTS

In fiscal year 2005, the Department's performance highlights in support of Service goals and objectives include the following:

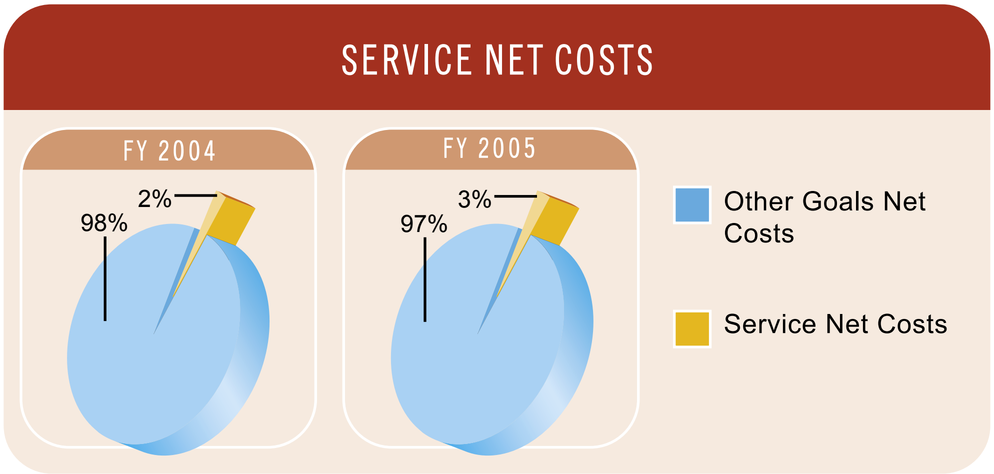
- The Department increased productivity, refined processes and automated services, and significantly reduced the backlog of applications for immigration services and benefits from approximately 3.8 million cases in January 2004 to approximately 1 million in September 2005. USCIS' goal is to eliminate the backlog of applications for immigration services and benefits, and establish a universal six-month or less processing time by September 30, 2006.
- On average, on an annual basis, USCIS:
  - Processes more than 6 million applications;
  - Serves more than 14 million customers via the National Customer Service Call Centers;
  - Serves approximately 5 million customers through information counters at local offices;
  - Processes nearly 90,000 asylum cases;
  - Performs more than 100,000 refugee interviews; and
  - Conducts the naturalization of approximately half a million new citizens.
- In the aftermath of Hurricane Katrina, USCIS offices nationwide were opened to displaced customers from the Gulf Coast to expedite replacement of immigration documents and rescheduling of Naturalization ceremonies.
- The USCG evaluates how well the Aids to Navigation (AtoN) system prevents collisions, allisions and groundings (CAG) by comparing results from the current period to those of previous periods. The Ongoing Vessel Traffic Service (OVTS), waterways management improvements and continuous maintenance of existing visual and radio aids to navigation system have contributed to a steady decline in CAGs.

- The Office of Immigration Statistics (OIS) in the Management Directorate is the nation's premier source of immigration statistics. This year OIS redesigned its website to improve customer access to high quality, user-friendly statistical immigration information.

TRENDS



The Net Costs of this goal in fiscal year 2005 was $1,838 million, or approximately 3 percent of the total Net Costs of the Department's Directorates.



To assess the achievement of all goals, we used quantitative performance measures with targets. These targets were contained in the performance-based budget submitted to Congress. A summary of our fiscal year 2005 performance against those targets is provided in the following scorecard. We report baselines that were successfully established as Target Met in the charts and tables in this section.

PERFORMANCE SCORECARD

Strategic Goal 6 - Service

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Screening Coordination and Operations	Enable Federal Immigration and Border Management agencies to make timely and accurate risk and eligibility decisions through coordination of screening capability policies, business strategy and processes, data, information systems, and technology to further enhance security and immigration, travel, and credentialing experiences.	0%	▼	247
Backlog Initiative	To support the processing of immigration and citizenship benefits.	0%	▼	248
Asylum and Refugee Services	Adjudicate asylum and refugee applications in a timely, accurate, consistent, and professional manner.	100%	▲	249 - 250
Immigrant Services	Provide legal permanent residency information and benefits in a timely, accurate, consistent, courteous and professional manner.	100%	◀ ▶	251
Naturalization Services	Provide citizenship and naturalization benefits in a timely, accurate, consistent, courteous, and professional manner.	0%	▼	252
Nonimmigrant Services	Provide temporary residency information and benefits in a timely, accurate, consistent, courteous, and professional manner.	100%	◀ ▶	253
Aids to Navigation	Eliminate collisions, allisions and groundings by vessels on our Nation's oceans and waterways.	100%	◀ ▶	254
Ice Operations	Maintain operational channels for navigation, limiting channel closures to two days per year (during average winters) and eight days per year (during severe winters).	100%	▲	255

* The Performance Goals in the Scorecard are shown as they were stated in the fiscal year 2005 performance plan, but where the goal has been improved, the new goal is shown. Both the old and new goals are shown in the Performance Information tables in Section II of this report. Some goals have been improved to better reflect intended program outcomes.

FUTURE STEPS

The United States will continue to welcome legitimate visitors and those seeking opportunities within our nation, while preventing terrorists and their supporters from entering the country.

During the next five years, the Department will establish clear lines of responsibility and authority in citizenship and immigration services to eliminate burdensome management and support functions. We will modernize immigration services by restructuring our business processes, implementing electronic filing and conducting virtual adjudications. These changes will eliminate backlogs and achieve the President's goal of processing immigration applications in six months or less.

To support the United States' humanitarian commitment, we will establish a Refugee Corps that will provide a strong and effective overseas refugee-processing program able to fulfill the U.S. Refugee Program's humanitarian objectives and more efficiently identify inadmissible people and those who are of national security interest.

We will work with the international trade community to facilitate and improve the flow of trade without compromising homeland security. The Automated Commercial Environment (ACE) will: use information technology to address increasing trade volume and changing trade requirements; improve the Department's data-gathering capability; and streamline the filing process and reduce the paperwork burden by eliminating multiple, redundant filings required by Federal agencies. We will continue to use risk-assessment tools to more effectively allocate resources to allow maximum use of staffing and minimize customer inconvenience while ensuring adequate safeguards. To facilitate lawful travel and immigration, CBP will implement a new design of its facilities starting in airports around the United States to integrate the border functions. The plan calls for combining CBP primary and secondary inspections into one. As a result, the majority of the traveling public will have less contact with CBP Officers allowing them to devote more time to those who are deemed higher risk. This will result in the better use of personnel, equipment and technology.

SUCCESS STORY

USCIS conducted the first overseas military Naturalization ceremonies since the Korean War. USCIS waived processing fees for members of the Armed Forces and made it easier for qualified military personnel to become citizens. Before October 1, 2004, active duty service members could only naturalize while in the United States. In all, more than 1,000 active duty service members took the Oath of Allegiance and became U.S. citizens while serving in Afghanistan, Kuwait, Germany, Iraq, Italy, Korea and Japan.

Strategic Goal 7 ⋆ Organizational Excellence

Value our most important resource, our people. Create a culture that promotes innovation, mutual respect, accountability and teamwork to achieve efficiencies, effectiveness and operational synergies.

Objective 7.1	Value our people.
Objective 7.2	Drive toward a single Departmental culture.
Objective 7.3	Continually improve our way of doing business.

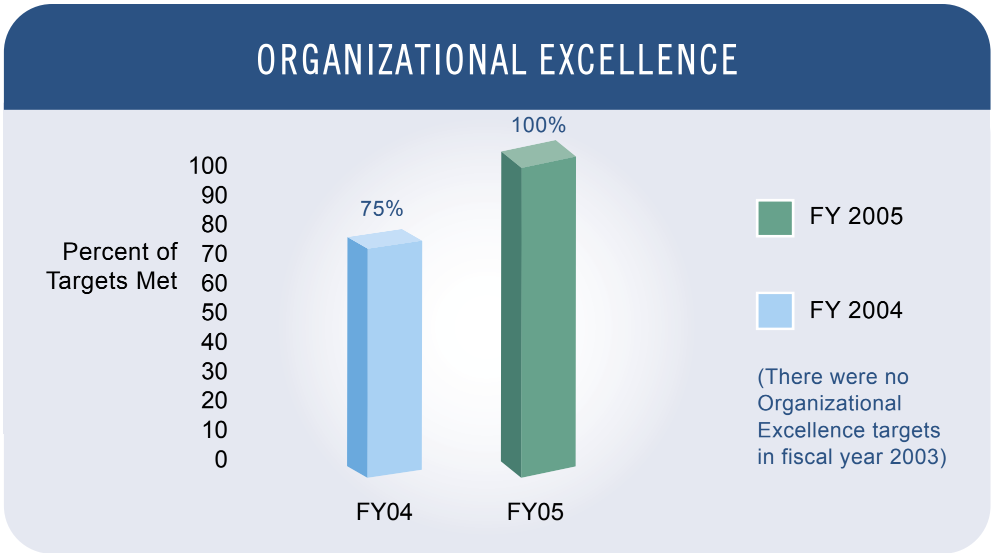
HIGHLIGHTS

In fiscal year 2005, the Department's performance highlights in support of Organizational Excellence goals and objectives include the following:

- USCG instituted the Unit Leadership Development Program, aimed at training and developing our next generation of leaders in the places they can be found accomplishing our missions: on our cutters, small boats and hanger-decks, or in our command centers, machine shops and offices. The program contains initial leadership competency-based learning activities, a crew survey, action plan job aid and an automated system of individual development plans for personnel.
- The CIO competed, evaluated, and awarded over fifteen pilot projects which demonstrate the latest advances in security, information-sharing, wireless, and geospatial technologies. This office also completed the Information Technology Infrastructure Transformation Program plan that consolidated 16 component data centers into two department-wide data centers to provide required availability and survivability; consolidated eight component Sensitive-But-Unclassified data networks into "OneNet" along with the Network and Security Operating Centers; and deployed a department-wide electronic mail solution.
- The Department continues making strides toward a single culture by creating seamless links between components. For example, on May 8, 2005, ICE agents at the land border port of Lewiston, N.Y., arrested David Kricheli, a native of the Republic of Georgia who was wanted for murder in Germany. Cross referencing existing US-VISIT fingerprints with Interpol fingerprints revealed that Michael Tonia, a Canadian truck driver and frequent border crosser, and Kricheli were the same person, enabling the arrest of this dangerous fugitive. ICE access to, and use of US-VISIT information was key to the success of this case.
- The new CBP Advanced Training Center, in Harpers Ferry, West Virginia, provides critically needed, state-of-the art training for our dedicated Federal law enforcement professionals. The preparation that officers and agents receive at the center will better equip them to keep the U.S. borders safe and secure. The center includes a Defensive Tactics Training Center; practi-

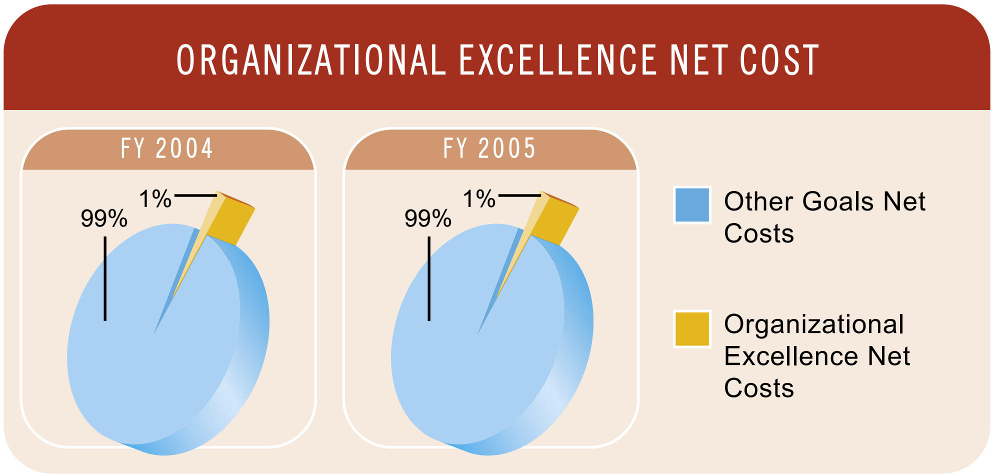
cal exercise environments: land border, airport arrival, urban hotel and warehouse; an armory; an administrative building with an auditorium, eight classrooms, a computer lab and library; and a Welcome Center. A firing range complex, situated to minimize environmental impact, is under development.

TRENDS


ORGANIZATIONAL EXCELLENCE

(There were no Organizational Excellence targets in fiscal year 2003)

The Net Costs of this goal in fiscal year 2005 was $621 million, or approximately 1 percent of the total Net Costs of the Department's Directorates.


ORGANIZATIONAL EXCELLENCE NET COST

To assess the achievement of all goals, we used quantitative performance measures with targets. These targets were contained in the performance-based budget submitted to Congress. A summary of our fiscal year 2005 performance against those targets is provided in the following scorecard. We report baselines that were successfully established as Target Met in the charts and tables in this section.

PERFORMANCE SCORECARD

Strategic Goal 7 - Organizational Excellence

Program	Performance Goal	Percent of Targets Met	Performance Trend from FY 2004	Detail Found on Page
Audit, Inspections, and Investigations Program	Ensure the integrity of DHS operations by conducting independent assessments of programs' efficiency and effectiveness.	100%	N/A	256
Counterterrorism Fund	Ensure that operating entities of the Department and other Federal agencies are promptly reimbursed for authorized unforeseen expenses arising from the prevention of or response to terrorist attacks.	100%	◄ ►	257
Office of the Chief Information Officer	The Department of Homeland Security components and stakeholders have world-class information technology leadership and guidance enabling them to efficiently and effectively achieve their vision, mission and goals.	100%	◄ ►	258
Office of the Secretary and Executive Management	Maximize management efficiencies and ensure continuity of services by consolidating DHS support services.	100%	◄ ►	259

* The Performance Goals in the Scorecard are shown as they were stated in the fiscal year 2005 performance plan, but where the goal has been improved, the new goal is shown. Both the old and new goals are shown in the Performance Information tables in Section II of this report. Some goals have been improved to better reflect intended program outcomes.

FUTURE STEPS

An agile and effective Department is essential to the rapid implementation of homeland security priorities, policies and objectives. We are establishing processes to identify and establish competitive standards and performance measures and, when appropriate, will recruit and retain the best people to provide effective and efficient services that ensure American citizens get the most value for their tax dollars. The Department will continue to communicate critical budget, cost and performance information to ensure stakeholders are informed, reasonable standards are set, and our people remain focused on getting the job done. We will maintain continual and unquestionable accountability and responsibility to ensure the effective use of resources allocated to the Department.

All elements of the Department will continue to ensure the core principles of organizational excellence are incorporated into our planning, programming and budgeting plans. During the next five years, our recapitalization efforts will include modernization that retains needed structure with enhanced capacity.

We will continue to work with our Federal, state, local and private-sector partners to invest in areas critical to achieving our mission, where our required capability is inadequate, performance is not competitive with alternatives sources or where technology offers the prospect of decisive, transformational improvement in capability. Specific emphasis will be placed on eliminating systems where technology is obsolete or redundant, the usage rate is low, or the contribution to mission effectiveness is suspect or minimal. We are coordinating our workforce weaknesses and skill gaps with our E-Gov requirements and with our competitive sourcing schedules and opportunities. We will also continue implementing a unified, modern, performance-based personnel system and will educate and train homeland security professionals and our partners.

Significantly improved budget, performance and financial integration is key to the success of this effort. Managers must understand the full cost of their operations to the taxpayer and their level of competitive performance. This information will lead to better decision making in the allocation of resources, and we are working to move from periodic analysis to a daily and project-by-project capability.

SUCCESS STORY

Every day thousands of dedicated Department of Homeland Security staff work hard to integrate and coordinate many legacy processes inherited from the original 22 agencies. By capturing its best practices, the Department constantly improves its effectiveness and efficiency. Staff members are pictured discussing how to improve the process of integrating the wealth of information that is included in the Department's performance and accountability report.

Other Management Information, Initiatives, and Issues

The Department of Homeland Security addressed a wide range of challenges in fiscal year 2005. It defended the country against terrorism and prepared for and responded to the natural disasters that devastated a whole region of our nation. The Department has reaffirmed the necessity to excel in all aspects of Homeland Security.

The Department is applying the lessons learned regarding Hurricane Katrina and other experiences to consistently and proactively ensure we move forward intelligently and effectively to fulfill our mission and vision. While this report focuses on the Department's performance goals, measures and financial performance, we also strived to improve every aspect of management of this large and complex organization. To that end, the Department's management achieved wide-ranging success throughout fiscal year 2005. The following highlights represent just a few of those successes. The Department:

- Continued to improve the accuracy and timeliness of consolidated financial statement submissions through the use of the Department of Treasury's Information Executive Repository and CFO Vision Software. The Department also continued mapping CFO Vision Software to ensure departmental financial statements are prepared in accordance with applicable accounting standards. Analytical, abnormal balance, desk officer and financial statement checklist procedures were developed to ensure Department components are consistently interpreting U.S. Standard General Ledger and OMB requirements. Finally, the Department produced guidance to the components for the Department's *Performance and Accountability Report*.
- Consolidated 22 separate agency processes for advertising and transferring available excess personal property into one departmental process. Reusing excess property itself resulted in significant cost avoidance, including the transfer of one boat and several helicopters from the USCG to CBP saving approximately $5 million.
- Developed the National Information Exchange Model (NIEM) in conjunction with the Department of Justice to standardize Extensible Markup Language (XML) messages. This greatly facilitated information sharing within Federal, state, local and tribal governments.
- Linked the Department's Investment Management System (IMS) to the Future Years Homeland Security Program (FYHSP) ensuring that the financial data in IMS is the same as in FYHSP, which eliminates the need to fund certify the business cases as a separate step.
- Implemented the human capital functional integration directive including alignment of human capital goals with strategic plan priorities.
- Became the first Agency/Department to satisfy the OMB's requirements for the establishment of a Strategic Sourcing Program. Strategic Sourcing Program savings to date are $112,020,608.
- Established a nationwide small business outreach program including Department of Homeland Security monthly events in the Washington, D.C., area and partnerships with other Federal agen-

cies, trade associations, and others to participate in various trade fairs around the country (many of which were congressionally sponsored).

- Created a Department-wide certification program for both contracting and program management personnel. Certification statistics include 73 percent of all contracting personnel certified and 132 program managers certified. We also created an online advance acquisition planning system for use throughout the Department.
- Established an integrated acquisition program and project process that provides needed oversight without burdensome and redundant processes. The initiative includes standing up an Integrated Project Review Team (IPRT) of subject matter experts.
- Developed Department-wide Resource Management Business Models that were incorporated into Version 2 of the Homeland Security Enterprise Architecture. These models were adopted by OMB as the baseline for the Financial Management Line of Business.
- Established an Internal Control Committee, which initiated a seven-step plan to prepare for the fiscal year 2006 audit of internal controls over financial reporting and completed a comprehensive internal control assessment of the consolidated financial reporting process within the Office of the Chief Financial Officer.

Financial Highlights

During fiscal year 2005, the Department continued to improve financial management in many areas:

- Fiscal year 2005 proved to be a watershed year for internal controls government-wide and, in particular, at the Department of Homeland Security. Shortly after passage of the Department of Homeland Security Financial Accountability Act, the Department developed a strategy and vision for implementation. Most notably, the Department:
  - Established an Internal Control Committee (ICC) responsible for improving internal controls;
  - Issued a comprehensive Implementation Guide to comply with the Department of Homeland Security Financial Accountability Act;
  - Completed a comprehensive internal control assessment of the consolidated financial reporting process within the Office of the CFO.

- The Department continued to streamline its finance and accounting organization, bringing TSA from external cross-servicing by DOT Federal Aviation Administration to the USCG and absorbing the Federal Protective Service into ICE;

- The Department focused on reducing material weaknesses by instituting a comprehensive Corrective Action Plan process. Faced with the challenge of 18 material weaknesses inherited from its component agencies when it was formed, the Department has made significant progress in eliminating or consolidating material weaknesses to seven for fiscal year 2003 and 10 for fiscal year 2004. The increase in material weaknesses in fiscal year 2004 was due to an increase in audit coverage of components that had not been subject to that level of review at legacy agencies. The consolidation of material weaknesses in fiscal year 2003 was not a true baseline of where the Department was in fiscal year 2003, but rather a reflection of where the legacy organizations were when they became part of the Department.

- Based on the Department's functional integration effort to bring all experts under one integrated method of operation, a series of Management Directives were approved in October 2004, including the Financial Management Line of Business Functional Integration Management Directive. This management directive established the Department of Homeland Security authorities and responsibilities of the Office of the CFO. The directive is the principal document for leading, governing, integrating, and managing financial management functions throughout the Department.

- During the past year, CBP has made significant progress in the implementation of a critical financial systems' initiative as part of a continuing effort to modernize its financial systems. CBP's enterprise resource planning system solution, SAP, provides the tools for enhanced customer service and facilitates a shift in the role of finance from a transaction processing and record-keeping function to an analytic and integrated decision-making function. SAP Release 3, which went live in October 2004, addresses the areas of core finance, budget execution, and financial reporting and completes CBP's original vision for implementing this new system.

GRANTS MANAGEMENT

In the previous fiscal year, the Department issued a Management Directive, which required Department awarding offices to use the website Grants.gov FIND to post grant opportunities. Grants.gov is a government-wide clearinghouse that allows organizations to electronically find and apply for competitive grant opportunities from all Federal grant-making agencies. The Department has given the Office of Grant Policy and Oversight in the Management Directorate the responsibility to ensure that all grant award opportunity postings are in compliance with statute, regulations, executive orders and other government-wide mandates.

In addition to posting announcement synopses of funding opportunities on the website Grants.gov FIND, the Department began implementing awarding program activity in the Grants.gov APPLY part of the website during fiscal year 2005. A Grants.gov program participation schedule was developed, and the Department anticipates continuing to phase in its awarding office participation in the Grants.gov APPLY process over the next fiscal year and beyond.

Several of the Department's programs continue to be administered through outsourcing with other Federal agencies. IT support personnel from participating Department grant awarding offices with a pre-existing grant management system and the Grants.gov program office will work together throughout fiscal year 2006. These offices will test a system-to-system interface between their respective IT systems to facilitate use of the Grants.gov APPLY process as a one-stop public resource. The Department continues to coordinate with the Grants.gov program office and Department of Homeland Security awarding offices to expand use of the Grants.gov system. The ultimate goal is to make departmental grant awards, cooperative agreements, and other forms of assistance readily available to the public.

WORKING CAPITAL FUND

The Department's Working Capital Fund (WCF) is a revolving fund, established in fiscal year 2004, pursuant to Section 506, Public Law 108-90. The WCF presents the Department with the opportunity to apply best practices from the public and private sectors for improving organizational performance and operational efficiencies, and promotes full recovery of goods and services for selected agency-wide programs, activities and services. The WCF has made considerable expansion in fiscal year 2005. The budget for the WCF increased from $107,340,396 and 29 activities in fiscal year 2004 to a budget of $301,246,000 and 57 activities in fiscal year 2005. This expansion reflects including the recurring and new activities in the WCF. The activities are organized under the four categories listed below:

Fee for Service Activity – Fee for Service is the costs for operating the "business." The costs are reimbursed by billing customers for the provision of goods and services, through rates that are pre-approved by the CFO and reviewed by component customers; therefore, each Fee for Service Activity is expected to recover is operational costs.

Government-Wide Mandated Service Activity – The activities may or may not provide a direct or indirect benefit to the component assessed. Examples are the government-wide e-Government activities related to the PMA.

Department of Homeland Security Crosscutting Activity – The Department of Homeland Security Crosscutting Activities are Department-wide programs. The actual costs of the programs are recouped by redistributing the costs to the components based on their share of the discretionary budget, staffing or some fair and equitable pro-rata basis.

WCF Management Activity – The WCF Management Activity includes the funding for the staff that develops WCF policy and procedures, formulates and executes the WCF budget, and resolves disputes between activity managers and customers.

For continued expansion, the most important initiative of the WCF for fiscal year 2005 was to improve its internal operations. First, this means getting the WCF budget cycle in synchronization with the appropriated budget request. Second, continue folding into the WCF common administrative services so that changes against components are consolidated. Third, improve the cost methodology for determining customer assessments for products and services received. In addition, the WCF staff has implemented monthly Activity Managers meetings and quarterly Customer/Activity Managers meetings to address budget execution and budget formulation issues and to communicate goals and strategies throughout the Department, while ensuring fiscal responsibility and accountability, as the Activity Managers strive to reach activities goals and objectives.

In fiscal year 2005, the primary goal in accomplishing our mission was to implement policies and procedures as tools to help the Activity Managers achieve results, safeguard the integrity of their activities, and to ensure the effectiveness and efficiency of day-to-day operations. The WCF will continue all functions and activities from fiscal year 2005 in fiscal year 2006, while providing more technical assistance to all WCF Activity Managers and customers components to achieve optimum use of scarce departmental resources. Activity increases for fiscal year 2006 is due to the incorporation of the Tri-Bureau shared services activities into the WCF. Continued activity increases will ensure that the Department can provide centralized administrative services at a savings to the components that participate in the WCF.

BANKCARD PROGRAMS

The chart included below summarizes the business accomplished through the Department's bankcards since the program's October 1, 2003, inception. With more than $1 billion spent in more than 6 million transactions, the Department's dependence on these cards has increased steadily during fiscal year 2005. For example, September 2005 purchase cardholders spent more than $75 million that included purchases in support of the mission of the Department and aid in the Gulf Coast hurricane disaster effort.

BANKCARD PROGRAMS

Bank	US Bank	Citibank	Bank One
Business Line	**Purchase**	**Travel**	**Fleet**
Cards Holders	13,907	123,880	33,464
Transactions	1,123,435	2,704,465	2,188,024
Dollars Spent	$435,031,126	$516,739,002	$101,432,117
Refunds	$7,997,534	$631,631	$84,000

Purchase Card – A contractor-issued government charge card for use by Department employees to purchase goods and services that cost less than $2,500. The purchase card is the preferred method for buying goods and services less than $2,500.

Travel Card – A contractor-issued government charge card for use by Department employees authorized to travel to pay for lodging, meals and transportation costs. Cardholders pay their bills by reimbursement through the voucher process.

Fleet Card – A contractor-issued government charge card for use by Department employees to purchase fuel, emergency repairs, toll passes and fluid for mobile assets such as vehicles, vessels, aircraft and other equipment. It may also be used to acquire bulk fuel under contract by the government or through commercial sources.

A refund is a monetary payment provided by charge card vendors to agencies. The three types of refunds are: Sales – payments from the charge card vendor to the agency based on the dollar or "spend" volume during a specified time period; Productivity – payments from the charge card vendor to the agency based on the timeliness and/or frequency of payments to the vendor; and Corrective – payments from the charge card vendor to the agency to correct improper or erroneous payments or an invoice adjustment.

Management Assurances

INTRODUCTION

A number of laws require agencies to establish internal controls and financial systems that reasonably assure the integrity of Federal programs and operations. These laws also require that the head of the agency, based on an evaluation, provide annual Assurance Statements regarding whether the agency met the requirements. The Department evaluated its internal control, financial management and information security systems for fiscal year 2005. To identify and qualify material weaknesses, we used the following criteria:

- Significantly impairs the fulfillment of the Department's mission;
- Deprives the public of needed services;
- Significantly weakens established safeguards against waste, loss, unauthorized use or misappropriation of funds, property, other assets or conflicts of interest;
- Merits the attention of the Secretary, the President or a relevant Congressional oversight committee;
- Conformance to government-wide systems requirements; and
- Completeness and reliability of performance data.

In addition, The Department of Homeland Security Financial Accountability Act requires a separate assertion of internal control over financial reporting. The financial reporting assertion is reported as a subset to Section 2 of the Federal Managers' Financial Integrity Act. A material weakness pursuant to the Department of Homeland Security Financial Accountability Act is defined as a reportable condition or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements or other significant financial reports, will not be prevented or detected.

U.S. Department of Homeland Security
Washington, DC 20528

SECRETARY'S MANAGEMENT ASSURANCES

The Department of Homeland Security is committed to developing a culture of integrity, accountability, and excellence in all we do. The Department's management is responsible for establishing and maintaining effective internal control over the three internal control objectives of effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. In addition, the safeguarding of assets is a subset of these objectives. In accordance with the Financial Managers' Financial Integrity Act, the Department of Homeland Security Financial Accountability Act, and the Reports Consolidation Act, I have directed an evaluation of the internal control at the Department of Homeland Security in effect during the fiscal year ended September 30, 2005. This evaluation was conducted in accordance with OMB Circular No. A-123, *Management Accountability and Control*, Revised June 21, 1995, and GAO's *Standards for Internal Control in the Federal Government*. Based on the results of this evaluation and assurances provided by Component Heads, the Department provides the following assurance statements.

Reporting Pursuant to the Federal Managers' Financial Integrity Act, Section 2 and the Department of Homeland Security Financial Accountability Act

Based on information provided, the Department of Homeland Security provides reasonable assurance as to the overall adequacy and effectiveness of internal controls, except for internal controls over financial reporting as described in the paragraph below, and the following material weaknesses, as more specifically reported by the GAO High Risk Series:

- Implementing and Transforming the Department of Homeland Security; and
- Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security.

The Department of Homeland Security is unable to provide reasonable assurance that internal control over financial reporting was operating effectively. The following material weaknesses were found:

- Financial Management Oversight of Components;
- Financial Reporting Process;
- Financial Management Systems Functionality and Information Technology;
- Reconciling Fund Balances with Treasury;
- Accounting for Property, Plant, and Equipment;
- Accounting for Operating Materials and Supplies, and Seized Property;
- Accounting for Undelivered Orders, Accounts and Grants Payable, and Disbursements;
- Valuation of Actuarial Liabilities;

- Budgetary Accounting; and
- Reconciling Intragovernmental and Intradepartmental Balances.

Reporting Pursuant to Federal Managers' Financial Integrity Act, Section 4

The Department of Homeland Security's financial management systems do not substantially conform to government-wide requirements. The following non-conformances were found:

- Federal Financial Management Systems Requirements;
- Federal Accounting Standards;
- Noncompliance with the Standard General Ledger; and
- Not all financial management systems are fully certified and accredited in accordance with the Federal Information Security Management Act.

Reporting Pursuant to the Reports Consolidation Act

Based on information provided, the Department of Homeland Security's performance data used in the Performance and Accountability Report is complete and reliable, except for the following material inadequacies that were found within the reporting of fiscal year 2005 actual results against annual targets for the following programs:

- Biosurveillance;
- Fire Act Program; and
- Interoperability & Compatibility.

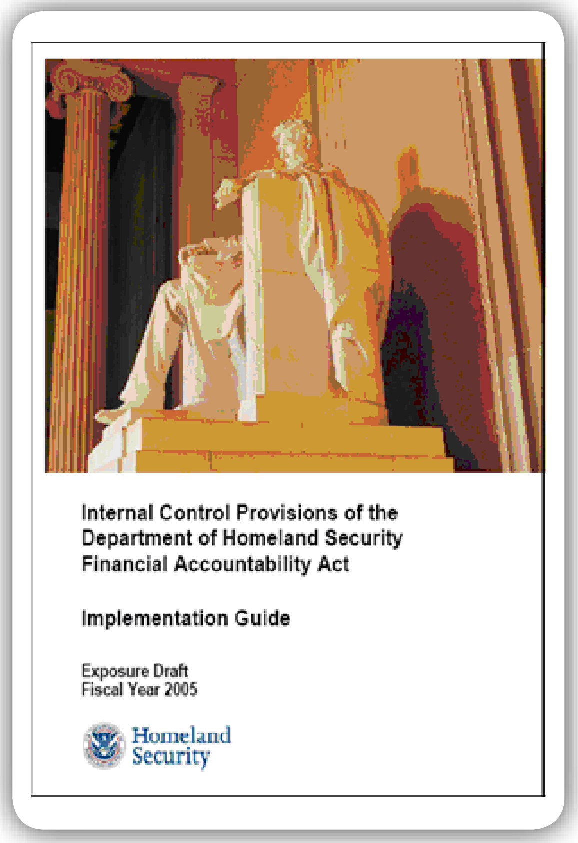
The Department of Homeland Security is unable to provide an assertion for the completeness and reliability of financial data used in the Performance and Accountability Report, as reported above for internal controls over financial reporting.

Michael Chertoff
Secretary Department of Homeland Security

INTERNAL CONTROL COMMITTEE

Fiscal year 2005 proved to be a watershed year for internal controls at the Department. Shortly after passage of the Department of Homeland Security Financial Accountability Act, the Department developed a strategy and vision for implementation. Most notably, the Department established an Internal Control Committee (ICC) responsible for improving internal controls. ICC membership includes a Senior Management Council, an ICC Board, and a Senior Assessment Team. The Senior Management Council is comprised of the Department's Under Secretary for Management, Chief Administrative Services Officer, Chief Financial Officer, Chief Human Capital Officer, Chief Information Officer, and Chief Procurement Officer. Their function entails overall management accountability, monitoring of corrective action plans, and ICC sponsorship. The ICC Board seeks to integrate and coordinate internal control assessments with other internal control-related activities and includes representatives from all Department lines of business to address crosscutting internal control challenges. Finally, the Senior Assessment Team, comprised of senior level financial managers, carries out and directs component level internal control assessments. Over the past year the ICC has:

- Published our landmark implementation guide, which is specifically tailored to support an attestation on internal control over financial reporting as required by the Department of Homeland Security Financial Accountability Act.
- Developed a comprehensive integrated framework for the Federal Managers' Financial Integrity Act and took significant steps to prepare for implementation of the recent revisions to OMB Circular No. A-123, *Management's Responsibility for Internal Control*, effective in fiscal year 2006.
- Implemented the GAO *Internal Control Management and Evaluation Tool* across the Department to facilitate the development of internal control activities in accordance with GAO's *Standards for Internal Control in the Federal Government*.
- Initiated a seven-step plan to prepare for the fiscal year 2006 audit of internal controls over financial reporting.
- Completed a comprehensive internal control assessment of the consolidated financial reporting process within the OCFO. In addition, the USCG, one of our largest components, has initiated process level documentation pilots.
- Developed corrective action plans for all material weaknesses and reportable conditions and a Management Directive and Process Guide to ensure these corrective action plans demonstrate results.



Internal Control Provisions of the
Department of Homeland Security
Financial Accountability Act

Implementation Guide

Exposure Draft
Fiscal Year 2005

Homeland
Security

MANAGEMENT PLANS, CORRECTIVE ACTIONS AND NON-COMPLIANCES WITH LAWS AND REGULATIONS

CORRECTIVE ACTION STATUS

Figure 1 presents a chart of Material Weaknesses, Reportable Conditions and Non-Compliances with Laws and Regulations which the Department identified and reported from the inception of the Department in fiscal year 2003 through fiscal year 2005. During fiscal year 2005, one new material weakness was identified, two existing material weaknesses were combined, one reportable condition was downgraded and three new non-compliances with laws and regulations were identified. The three new non-compliances with laws and regulations were for the: *Federal Financial Management Improvement Act of 1996, Government Performance and Results Act* and *Department of Homeland Security Financial Accountability Act.*

FIGURE 1

Status of Financial Statement Audit Findings

	Legacy Components Pre-FY 2003	FY 2003	FY 2004	FY 2005
Material Weaknesses	18	7	10	10
Reportable Conditions	12	7	3	2
Compliance with Laws and Regulations	1	3	4	7
Total	31	17	17	19

OMB Circular No. A-123, *Management's Responsibility for Internal Control*, requires that each agency identify and report on the most critical material weaknesses affecting the agency. The Department has adopted the high-risk designations recommended by the GAO to better focus on the major challenges of the organization. Department staff and senior management officials continuously monitor corrective action progress for all material weaknesses and reportable conditions. The resolution of these weaknesses, as well as the self-identified internal control weaknesses, reportable conditions and non-compliance findings reported in the fiscal year 2005 financial statements are presented in the following tables.

The Department has established a corrective action planning process for remediating corrective actions for material weaknesses, reportable conditions and non-compliance findings. While the Department made progress in correcting material weaknesses reported in the fiscal year 2004 financial statement audit, delays in completing corrective actions in some components and a re-base-lining of several multiyear corrective action plans precluded the achievement of critical milestones originally scheduled for completion in fiscal year 2005.

CORRECTIVE ACTIONS

FMFIA Section 2 Material Weaknesses as of September 30, 2005

Title: Implementing and Transforming the Department of Homeland Security
Entities: Department
Originally Reported: GAO-05-207
Target Date: Fiscal Year 2007

Description:

For the Department to successfully address its daunting management challenges and transform itself into a more effective organization, it needs to (1) develop a department-wide implementation and transformation strategy that includes comprehensive threat and risk assessment and strategic management principles to set goals and priorities, focus its limited resources, and establish key milestones and accountability provisions; (2) develop adequate performance measures and evaluation plans; (3) provide sound and innovative human capital management; and (4) follow through on its corrective actions to address management, programmatic, and partnering challenges.

Corrective Actions:

Concurrently, the Department is initiating corrective actions on a broad array of programmatic challenges that require sustained effort. These challenges include improving transportation, cargo, and border security; systematically tracking visitors; consolidating border security functions; updating outmoded capabilities in the USCG fleet; and balancing homeland security with other missions, such as law enforcement and disaster planning. Also, the Department's progress in forming effective partnerships with other governmental and private-sector entities remains challenged in several critical areas, such as improving critical infrastructure protection and emergency preparedness, communication among first responders, dissemination of timely and specific threat information, and planning for continuity of operations in case of an adverse event.

Fiscal Year 2005 Progress:

With the advent of the Second Stage Review (2SR) the Department has put forth a six point plan to transform the Department into a more effective organization with robust planning, management, and operations while maintaining and improving readiness for its highly critical mission to secure the homeland. Five of the six 2SR points include initiatives to:

- Strengthen border security and interior enforcement and reform immigration processes;
- Enhance information sharing with our partners;
- Improve the Department's financial management, human resource development, procurement, and information technology;
- Realign the Department's organization to maximize mission performance; and
- Implement and transform the Department of Homeland Security.

Title: Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security
Entities: Department
Originally Reported: GAO-05-207
Target Date: Fiscal Year 2007

Description:

Recent federal law and policy changes established requirements for information-sharing efforts, including the development of processes and procedures for sharing intelligence, law enforcement, immigration, critical infrastructure, first responder, and other homeland security related information. However, the required policies and procedures are still being developed and need to be consistently and effectively implemented. The Department has not established processes and procedures for disseminating homeland security information to the private sector.

Corrective Actions:

To address potential barriers to information sharing, strategies have been developed to address information sharing challenges, including: (1) establishing clear goals, objectives, and expectations for participants in information sharing efforts; (2) consolidating, standardizing, and enhancing federal structures, policies, and capabilities for the analysis and dissemination of information, where appropriate; and (3) assessing the need for public policy tools to encourage private-sector participation.

Fiscal Year 2005 Progress:

The Secretary's Second Stage Review includes a sixth initiative to establish appropriate and effective information-sharing mechanisms to improve Homeland Security.

Department of Homeland Security FAA Material Weaknesses as of September 30, 2005

Auditor Identified Material Weaknesses in Internal Controls Over Financial Reporting

Title: Financial Management and Oversight
Entities: Department, ICE, USCG
Originally Reported: FY 2003 (Department), FY 2004 (ICE), FY 2005 (USCG)
Target Date: 9/30/2006

Description:

Note: This material weakness is a combination of two fiscal year 2004 material weaknesses - (A) Financial Management Structure and (B) Financial Management and Oversight at ICE.
ICE did not correct any conditions reported in fiscal year 2004 and incurred new findings. Financial management at ICE continues to be ineffective and requires significant assistance from the OCFO. ICE: (1) lacked a sufficient number of qualified managers and staff to perform its accounting responsibilities; (2) lacked a strategy to identify root causes of errors and correct deficiencies; (3) continued to operate unreliable processes which resulted in material errors, irregularities and abnormal balances; (4) executed administrative and accounting functions for other Department components without proper reimbursable agreements; and (5) was unable to record correcting adjustments to restate the fiscal year 2004 financial statements for known errors.

USCG: (1) did not fully implement a financial management organizational structure that ensures complete and accurate data to support financial statement assertions; (2) did not establish clear management oversight for adjustments to account balances; and (3) did not fully establish management oversight and provide accounting operational guidance to other offices and facilities within USCG.

The OCFO: (1) has not fully completed the build-out of the OCFO; (2) provided effective management and oversight to ensure that: (a) component corrective action plans are developed, implemented, tracked and completed, (b) that component financial management and reporting problems are promptly and effectively addressed, (c) the separation of workload among OCFO staff allows for proper supervisory reviews, and provides appropriate back-up for key staff, and (d) processes are implemented to draft a timely, accurate and complete PAR and accurate monthly financial statements.

Corrective Actions:

The OCFO will use contractor and staff to prepare standard financial management operating policies and procedures; complete an internal control framework for financial management; evaluate internal controls over financial reporting, identify risks; and create an inventory of internal control issues.

ICE will update an inventory of financial policies and procedures. The Department and ICE will transition legacy financial data to ICE. ICE will establish an office to ensure that agreements are obtained timely and to track performance. Funds are requested to hire 14 staff to address data integrity issues. A contractor will complete a study of financial management.

Fiscal Year 2005 Progress:

The OCFO hired and contracted accountants, auditors and senior financial managers who, collectively, address the staffing deficiencies. The OCFO established Desk Officer reviews which address accounting and reporting issues including eliminations, abnormal balances, and Standard General Ledger (SGL) analytic issues. An Internal Control Committee including CXOs and program managers was set up early in the year. The GAO Internal Control Management and Evaluation tool based on the five essential elements of internal control was completed. ICE has made some progress in clearing up abnormal balances, eliminations, and SGL analytic issues. The USCG was added as a new finding in fiscal year 2005.

Title: Financial Reporting
Entities: Department, EP&R, ICE, SLGCP, TSA, USCG
Originally Reported: FY 2003
Target Date: 9/30/2007

Description:

The OCFO: (1) was unable to prepare a balanced consolidated financial statement until November 2005; (2) has not fully documented policies and procedures for many critical financial reporting processes; (3) has not ensured that monthly TIER submissions were prepared timely and accurately; and (4) did not require components to use TIER analytical tools and accepted explanations from components for financial statement abnormalities that were incomplete and inaccurate.

The USCG: (1) used a financial reporting process that required a significant number of "on-top" adjustments; also, TIER data is produced from a database that does not match the underlying transactions; (2) had significant abnormal balances; (3) routinely processed adjusting entries without verifying that ending balances were properly supported at the transaction level; (4) did not consistently document year-end closing entries; and (5) had poor design of some account reconciliation processes.

ICE has not: (1) established effective internal controls over the daily accounting and recording of transactions, supervisory review, reconciliation of accounts and documentation of supporting information for auditor review; (2) reconciled quarterly Treasury budgetary resource reports that could indicate a potential anti-deficient situation ; (3) designed some account reconciliations well; (4) provided guidance to Department-ICE components explaining how to process financial transactions timely and accurately; (5) submitted OCFO deliverables timely; and (6) successfully integrated Federal Protective Service accounting data from GSA.

TSA experienced difficulties in the monthly closing of its general ledger due in part to its change in accounting service provider. USCG, SLGCP, TSA and ICE did not accumulate cost data by strategic goal. TSA and FEMA did not document the full cost of each strategic goal. SLGCP has not ensured that their accounting provider can meet monthly TIER edits and is performing quality assurance work on financial statement and footnote disclosure data. FEMA's National Food Insurance Program (NFIP) contractor did not provide year end data timely.

Corrective Actions:

The OCFO will: (1) obtain additional staff to provide oversight and assist components; (2) lead the components in an assessment of internal controls over financial reporting; (3) update and communicate improved fiscal year 2005 PAR Guidance; (4) conduct TIER training; (5) develop monitoring controls to ensure that components comply with PAR financial reporting policies and procedures; (6) implement a process to prepare financial statements that fully complies with reporting standards; (7) provide instruction and management oversight of the FMFIA evaluation process; and (8) develop a method for reporting cost data by strategic goal.

Fiscal Year 2005 Progress:

The OCFO: (1) hired and trained new personnel; (2) developed an Internal Control Committee; (3) distributed updated fiscal year 2005 PAR Guidance; (4) issued an implementation guide to financial reporting; (5) developed an assessment for the Secretary's assurance statements and for FMFIA; (6) developed a project plan which inventoried and documented internal controls over financial reporting; (7) conducted an assessment of current financial reporting processes to reduce complexity and improve internal controls; and (8) cross trained staff to reduce reliance on a limited number of key personnel.

Title: Financial Systems Security
Entities: Department
Originally Reported: FY 2003
Target Date: 9/30/2007

Description:

Five component financial and feeder systems were not properly certified and accredited. Problems with system access security for hired and terminated employees. Lack of review of access rights to key financial systems. Missing or poor password controls. Poor systems security configurations. Changes to system configurations were not always documented. Audit log trackings were not always activated. Poor operating system controls. Incomplete segregation of duties and incomplete assignment of key security positions. Five components had incomplete or outdated business continuity plans and systems. Continuity plans were not adequately tested and training for emergencies was incomplete. Weak access and segregation controls associated with key Department financial applications.

Corrective Actions:

Audit Findings arising from OMB Circulars A-127 and A-130 have been consolidated into a single material weakness of the Department. Corrective Actions on these areas are addressed within the Department's FISMA process and corrective action plans are covered under the Plan of Action and Milestones (POA&M) required by the statute.

Fiscal Year 2005 Progress:

The Department achieved two significant milestones that will help the department move toward managing a successful information security program. First, the Department completed a comprehensive inventory of its major applications and general support systems, including contractor and national security systems, for all organizational components. Second, the Department implemented a department-wide certification and accreditation (C&A) tool that incorporates the guidance required to adequately complete a C&A for all systems. The completion of these two tasks eliminated two factors that significantly held the department back in achieving some success in establishing its security program in the last two years.

The Department issued the *DHS Information Security Program Plan of Action and Milestones (POA&M) Process Guide*, which provides the department and components with the necessary guidance and procedures to develop, maintain, report, and mature the POA&M process.

Title: Fund Balance with Treasury
Entities: ICE, USCG
Originally Reported: FY 2004
Target Date: 12/30/2006

Description:

ICE: (1) did not complete and lacked clear written policies to timely reconcile FBWT accounts; (2) did not timely and accurately clear items carried in suspense; and (3) was unable to obtain document level information for ICE-Components processed by legacy agencies.

USCG: (1) did not timely and accurately clear suspense items; and (2) did not maintain proper documentation to validate the accuracy of FBWT reconciliations and the clearing of suspense items.

Corrective Actions:

USCG will hire additional staff to handle FBWT reconciliation and document procedures for developing suspense reports and clearing suspense transactions older than 30 days. ICE will assemble a team with contractor support to tackle resolution of all outstanding items. ICE plans to hire additional personnel to work in this area.

Fiscal Year 2005 Progress:

ICE has assembled a FBWT reconciliation team, developed suspense backlog reports, and held conference calls with ICE offices to obtain proper supporting documentation. After conducting a pilot internal control assessment of FBWT in fiscal year 2005, USCG will develop a detailed plan, approach, priority list and schedule for budgetary and proprietary reconciliations during the first quarter of fiscal year 2006.

Title: Property, Plant, and Equipment
Entities: BTS (US-VISIT), USCG
Originally Reported: FY 2003
Target Date: 9/30/2007

Description:

USCG has not: (1) accurately, consistently, and timely recorded PP&E in its fixed asset system; (2) maintained proper documentation; (3) documented methodologies to support PP&E values not supported by original acquisition or other documentation; (4) implemented a proper tracking and tagging system; (5) developed an effective physical inventory process for repairable PP&E; and (6) properly accounted for improvements and impairments to buildings and structures.

The US-VISIT program did not consistently identify and capitalize software development costs or properly distinguish software in production from software in development.

Corrective Actions:

USCG will evaluate, develop, implement and validate existing controls. Alternative methodologies will be developed, evaluated, and tested to support the value of PP&E that lacks sufficient documentation. Documentation standards and retention policies will be reviewed and improved. Policy and procedures for performing physical inventories of repairable items will be updated. Accounting for improvements to buildings and structures will be reviewed for compliance with GAAP. Lease agreement procedures will be updated. ICE will review existing procedures on identifying and capitalizing software development costs and on recording software that is moved from development to production.

Fiscal Year 2005 Progress:

ICE has reviewed existing software capitalization policy and developed and implemented improved procedures.

Out of the total PP&E balance of approximately $5.9 billion has been reviewed and accepted by the auditors as adequate to support PP&E balances. During fiscal year 2005, USCG has made substantial progress in PP&E by presenting an additional $1.6 billion in asset value for audit review. The remaining $1.2 billion will be addressed in fiscal year 2006 and fiscal year 2007.

Title: Operating Materials and Supplies (OM&S), and Seized Property
Entities: USCG, USSS
Originally Reported: FY 2003
Target Date: 9/30/2007

Description:

USCG: (1) internal controls over physical counts at field locations were not operating effectively; (2) policies, procedures and controls for OM&S at Inventory Control Points (ICPs) were not completely implemented; and (3) processes and controls were not in place to fully support the calculated value of field held and ICP OM&S.

At USSS, the September reconciliation for seized currency was not completed timely (though earlier time periods were okay).

Corrective Actions:

USCG will update physical inventory policy and procedures for field units and Inventory Control Points (ICPs). Teams will conduct comprehensive field unit inventories. A monitoring website for field unit physical inventories will be developed. Location validation programs will be reviewed for adequacy of design. A risk-based cycle counting policy will be reviewed. Policy for documentation support and OM&S valuation will be updated.

Fiscal Year 2005 Progress:

USCG is preparing a plan to decrease the amount of OM&S on hand and to properly value and classify the remaining balance. Improvements have begun in fiscal year 2005 with $2.5 million in funding dedicated to this effort that is projected to require two years and additional funding to accomplish. Significant remediation includes rebalancing inventories, re-pricing on-hand quantities and disposing of excess inventory. The result will be a significant reduction in risk by implementing a major change in business practices in this area.

USSS has instituted new policy and procedures and all targets have been satisfied with the exception of the final implementation of the C&E system slated for 2007. The target date for completion of the C&E was changed due to funding and resources needed to develop and implement the system.

Title: Undelivered Orders, Accounts and Grants Payable, and Disbursements
Entities: FEMA, ICE, SLGCP, TSA, USCG
Originally Reported: FY 2003
Target Date: 9/30/2006

Description:

ICE has not: (1) ensured that invoices are paid timely and with proper documentation and that IPACs are cleared timely from suspense; (2) recorded S&T and IAIP disbursements made by legacy agencies timely; (3) prevented duplicate payments to vendors on prior year obligations for selected shared Treasury accounts; (4) properly liquidated open obligations; (5) adopted policies to verify and validate obligations performed by field personnel; (6) verified the accuracy of obligations created in PRISM and other ICE systems; and (7) implemented policies that require confirmation of receipt of goods and services prior to payment of invoices.

USCG did not: (1) ensure timely review and validation of undelivered orders (UDOs); (2) timely reconcile paid orders to FBWT disbursements; (3) lacked policies to ensure the timely recording of contract awards; (4) weakness with policies and procedures related to the Financial and Procurement Desktop (FPD); (5) fully implement a Procurement Management Effectiveness Assessment (MEA), an assessment tool for compliance with Federal statutes and regulations; and (6) fully document the process used to estimate accounts payable.

SLGCP did not resolve discrepancies underlying a year-end grants payable liability.

TSA: (1) was unable to support the accuracy and completeness of accounts payable and UDO balances; (2) had inadequate grant documentation; (3) along with FEMA and SLGCP, did not properly monitor compliance with the *Single Audit Act Amendments of 1996* and laws and regulations supporting *Audit Follow-up*; and (4) did not validate grant accrual methodology.

Corrective Actions:

Develop an enforcement mechanism to ensure that UDOs are reviewed on a quarterly. Review personnel assignments to ensure proper separation of duties. Improve UDO reports. Receive assurances that grantee reporting systems are certified and accredited. Hire personnel to perform oversight and monitor grant close out activities. Ensure that grantee application packages are maintained, performance reports are obtained, and OMB Circular A-133 requirements are met. Revise financial procedures to prevent duplicate payments across current and past accounting providers. Ensure that payments are made only after invoices are approved and evidence of the receipt of good or service is received. Complete disbursement testing to determine accurate accrual percentages. Issue memorandum instructing staff on proper procedures.

Fiscal Year 2005 Progress:

TSA obtained missing performance reports, payment approvals, and application packages for all managed grants. The Office of Acquisitions issued instructions mandating the use of the Central Contractor Registration (CCR) to verify the accuracy of all tax identification numbers. TSA has in combination with SLGCP implemented a process which ensures that all OMB Circular No. A-133 requirements are met by ensuring application packages are maintained, and performance reports obtained.

USCG and ICE have improved controls relating to processing obligations, improved segregation of duties, updated program logic in systems, revised instructions to oversee and monitor the contract acquisition process and reviewed and revised policies and procedures as necessary to correct the deficiencies.

Title: Actuarial Liabilities
Entities: USCG
Originally Reported: FY 2005
Target Date: 9/30/2006

Description:

USCG: (1) was unable to fully support its assertions relating to the accuracy and completeness of the underlying participant data, medical cost data, and trend and experience data provided to and used by the actuary for the calculation of its MRS and post-employment travel benefits liabilities; (2) did not follow established policies and procedures to accumulate data provided to and used by the actuary for computation of post-employment travel benefits; (3) did not perform periodic reconciliations between the medical expenditures subsidiary ledger and those recorded in the general ledger, which would have identified errors in the underlying data; and (4) did not have effective policies, procedures and controls to monitor the expenditures for medical services to ensure they are billed at proper rates and for valid participants only.

Corrective Actions:

USCG will: (1) develop and implement policy and procedures to include preventive and/or detective controls that support management's assertion of completeness, existence and accuracy of personnel data collected and provided to the actuary; (2) perform a thorough review of the spreadsheet used to record and monitor medical expenses to identify and correct any technical errors; (3) perform a periodic reconciliation between the medical expenditures recorded in the subsidiary ledger and records in the CAS and clearly identify reasons for variances in expenditures and undelivered orders; (4) conduct an update to the current Experience Studies to provide more accurate trending of USCG population experience, as recommended by USCG's actuary in their fiscal year 2003 and fiscal year 2004 reports; (5) establish and document specific procedures and internal controls to provide review and oversight of its actuarial firm to ensure that appropriate assumptions and data are used to develop the estimate for post-employment actuarial liabilities to include MRS and post-employment travel benefits; (6) perform a review of the annual headcounts provided by the PSC to the actuary, specifically by reconciling and resolving any discrepancies between the JUMPS payroll data to Direct Access personnel data to ensure completeness and accuracy; (7) verify that MTFs only bill for services provided to eligible USCG participants and sponsors; and (8) monitor medical care costs, including IBNR costs.

Fiscal Year 2005 Progress:

Not applicable, new finding.

Title: Budgetary Accounting
Entities: ICE (and Components), TSA, USCG
Originally Reported: FY 2004
Target Date: 6/30/2006

Description:

ICE (and ICE-Components): (1) control weaknesses might have allowed ICE to become anti-deficient; (2) obligations were not always recorded in a timely manner; (3) had an incomplete list of open obligations; (4) did not properly receive accounting records and responsibilities from legacy agencies; (5) had problems with obligations transferred between CBP and ICE; (6) did not have contracting officer approvals clearly documented on obligating documents; and (7) had inadequate controls over SF 132 and SF 133 (budgetary) reports.

USCG: (1) did not record post-employment permanent change of station (PCS) travel obligations timely; (2) did not use the validation and edit checks of the FPD; (3) did not properly interface FPD recorded obligation to the CAS; (4) had weaknesses in the system capabilities and controls over the recording of budget authority; (5) did not have controls to preclude the processing of procurement transactions by contracting officers with expired warrant authority; and (6) did not monitor commitments for aging or for timely release of funds.

The CAS used by TSA's accounting service provider could not record prior year de-obligations at the transaction level.

Corrective Actions:

ICE will: (1) replace collateral duty contracting officers with a small number of full-time contracting officers; (2) identify any obligations that were not recorded; (3) reconcile all items on SF 132/133 and make sure they are properly recorded; and (4) review suspense accounts for unrecorded items.

USCG will: (1) rely on the combination of new system edit checks and various non-system controls including FPD and CAS system enhancements of a specific "funds check" feature; (2) establish a methodology to determine the distribution of funds derived from the Oil Spill Liability Trust Fund for the Acquisition, Construction, and Improvements (AC&I) appropriation; (3) put in place strengthened controls for preventing contracting officers with expired warrant authority from conducting procurement transactions; (4) policy guidance will be added that requires all administrative target units to review commitments quarterly to ensure all commitments are valid, and executable; and (5) evaluate the costs and benefits of applying resources to exercise oversight of un-obligated commitments.

Fiscal Year 2005 Progress:

ICE: (1) pulled warrants of collateral duty contracting officers; (2) conducted reviews to identify and record unrecorded 2004 obligations; and (3) conducted reviews of suspense.

USCG: (1) revised controls and related policies and procedures to review and update the warrant authority of active contracting officers; and (2) developed and provided specific training related to any internal controls and related policy and procedure changes.

Title: Intragovernmental and Intradepartmental Balances
Entities: ICE (and Components), CBP, CIS, USCG
Originally Reported: FY 2003
Target Date: 9/30/2006

Description:

The Department did not reconcile intragovernmental balances with other Federal entities, especially the Department of Defense. The OCFO did not perform reconciliations throughout the year of all intragovernmental balances. ICE (and ICE components) and the USCG did not adopt effective SOPs or tracking systems. Intra-Department transactions between ICE, CBP, USCIS and other Department components did not eliminate correctly during the year. On-top adjustments were required at year-end.

Corrective Actions:

Develop reports that track intergovernmental transactions and create trial balances by trading partner. Dedicate an individual to reconciling and reporting Department governmental transactions. Review vendor table entries for Federal vendors for accuracy. Review existing obligating documents for accuracy. Improve documentation on inter-agency agreements and prevent mislabeling of components. Immediately charge back IPACs directed to the wrong component. Review financial reports for elimination related errors.

Fiscal Year 2005 Progress:

USCG implemented reports early in the year and has had clean intra-Department eliminations thereafter.

ICE completed the following five-part effort:

1) Reviewed the vendor tables to ensure that all Federal vendors are properly classified and that each has the correct trading partner code,

2) Obligated documents are reviewed and compared with the accounting system record to determine whether or not that it is linked to the correct vendor,

3) Ensured the Office of Procurement redouble its effort to issue interagency agreements and other obligating documents with proper billing instructions to reduce the widespread confusion between CIS and ICE exhibited by both internal offices and agencies external to ICE and CIS.

4) Mandated that incoming IPACs directed to the wrong Department agency be charged back to the originating agency with a notation that contains the correct Agency Locator Code. Currently, these IPACs are transferred to the correct Department agency. The IPAC then loses its original identity and tracking become a lengthy, labor intensive process. Expenditures between ICE and CIS become artificially inflated.

5) Created a Modification and Reconciliation Section to consolidate efforts and make corrections to the accounting system that will aid in the issuance of the error free financial reports. Previously, this function was spread among several units in the Office of Financial Management.

Auditor Identified Reportable Conditions in Internal Controls Over Financial Reporting

Title: Environmental Liabilities
Entities: CBP, S&T, USCG
Originally Reported: FY 2004
Target Date: 5/31/2006

Description:

At Coast Guard: (1) policies and procedures are not in place to identify, evaluate, and estimate potential environmental remediation of Coast Guard sites; (2) personnel do not always follow stated policies and procedures; (3) environmental liability estimates associated with lighthouses/light stations did not include soil testing assessment and remediation costs; (4) estimates for shore facilities and vessels were misstated; (5) consistent policies and procedures are needed to estimate remediation costs of specific projects, such as lighthouses and small arms firing ranges; and (6) no management review of year-end environmental compliance and remediation estimates.

At S&T, policies and procedures have yet to be developed to determine potential risk or accurately estimate an environmental liability for Plum Island.

CBP did not determine a year-end environmental liability until a review was performed in response to audit inquiry.

Corrective Actions:

USCG will develop guidance on the application of contingency factors for estimating environmental liabilities and develop a cost estimation model for environmental remediation of lighthouses. Estimation techniques for PCB removal costs on vessels will be simplified and improved. A revised Process Analysis Document (PAD) was created and utilized for the development of the fiscal year 2004 year-end vessel environmental estimates. The historical costs are developed for each type of vessel and starting in fiscal year 2005, this formula will be adjusted every 3 years to account for all written estimates released by the CG YARD. To be in compliance with SFFAS Number 6, paragraph 96, policies and procedures on the use of indexing will be implemented as applicable.

Fiscal Year 2005 Progress:

All units responsible for completing shore facilities environmental liabilities estimates at USCG have been directed to comply with existing policies dictated in Section 7.E of COMDTINST M71000.3C via memo 5200, dated 16Sep05 from CG-4. Specific procedures are currently under development and are expected to be released via incorporation in the Shore Asset Management System (SAM) SOP NLT end of 1st quarter fiscal year 2006.

CBP's finding is new for fiscal year 2005.

Title: Custodial Revenue and Drawback
Entities: CBP
Originally Reported: FY 2002
Target Date: 1/31/2009

Description:

For drawback: (1) the revenue accounting system, Automated Commercial Environment (ACE), lacked controls to detect and prevent excessive drawback claims and payments, necessitating inefficient manual processes to compensate; and (2) review policies were incomplete.

For the entry process: (1) outdated and poorly documented Compliance Measurement Program (CMP) policies and procedures produced inconsistent performance across ports of entry; (2) management identified weaknesses with CMP sample data that could affect the accuracy of the revenue gap disclosed in the CBP PAR; and (3) the CMP sample size was lower than in previous years.

For Bonded Warehouses (BWs) and Foreign Trade Zones (FTZs): (1) a lack of monitoring guidance and training; and (2) a CMP to measure the revenue gap and effectiveness of controls over trade compliance at FTZs and BWs.

Corrective Actions:

Automated Commercial Environment (ACE) will ensure that the drawback module includes all data elements needed for proper tracking and control. A statistician will develop a valid sampling methodology. Automating the in-bond process will allow for monitoring and tracking of in-bond shipments. It will also allow for the implementation of a new methodology to perform a complete review of imports included in drawback claims.

Fiscal Year 2005 Progress:

In-bond corrective actions for fiscal year 2005 have focused on issuing directives to standardize data submissions and mandate that all in-bond movements be presented electronically. CBP will then be able to implement a module in the Automated Commercial Environment (ACE) to electronically track and monitor in-bond shipments

Drawback specialists have been trained in the new methodology and it has begun to be use in fiscal year 2005 to process claims. Policies and procedures will be incorporated into an updated drawback handbook with automation to follow. Full implementation of ACE is now scheduled for September, 2009.

FMFIA Section 4 Material Weaknesses as of September 30, 2005

Title: Federal Financial Management Improvement Act of 1996 (FFMIA) Compliance
Entities: Department
Originally Reported: FY 2005 (New)
Target Date: FY 2007

Description:

The Department is not in compliance with Section 803(a) of the FFMIA which requires each agency to implement and maintain systems that comply substantially with: (a) Federal financial management system requirements, (b) Applicable Federal accounting standards, and (c) The Standard General Ledger (SGL) at the transaction level. This non-compliance was also noted in the Compliance and Other Matters section of the independent auditor's report.

Corrective Actions:

The Department will develop a comprehensive framework to ensure compliance with the requirements of FFMIA: (1) To implement and maintain systems that comply substantially with Section 803(a); (2) To require auditors to report on agency compliance with the three stated requirements as part of financial statement audit reports; and (3) To require a determination, based on the audit report and other information, whether their financial management systems comply with FFMIA. If they do not, to require development of remediation plans which will be filed with OMB.

Fiscal Year 2005 Progress:

The Department has completed the planning, risk and compliance assessment phase of the framework using the GAO Internal Control Management and Evaluation Tool. A self assessment of FFMIA compliance was performed using the results of the Tool as well as other GAO, OIG and IPA audit findings in the areas covered by OMB A-127 and A-130, resulting in a finding of non-compliance. With the receipt of fiscal year 2005 audit findings, the Department will develop a remediation plan to correct specific findings of non-compliance within the Department.

Title: Federal Information Security Management Act (FISMA) Compliance (Electronic Government Act of 2002)
Entities: Department
Originally Reported: FY 2004
Target Date: FY 2007

Description:

The Department is not in substantial compliance with FISMA that requires each federal agency to develop, document, and implement a department-wide program to provide information security for the data and information systems that support the operations and assets of the agency. Additional significant deficiencies have been found regarding the requirements of the Office of Management and Budget (OMB) Circular A-127 and Circular A-130, that executive agencies within the federal government: (1) Plan for security; (2) Ensure that appropriate officials are assigned security responsibility; (3) Periodically review the security controls in their information systems; and (4) Authorize system processing prior to operations and, periodically, thereafter. This non-compliance was also noted in the Compliance and Other Matters section of the independent auditor's report.

Corrective Actions:

Despite several major improvements in the Department's information security program, Department organizational components have not completely aligned their respective information security programs with the Department's overall policies, procedures, and practices. Thus, for example: (1) All Department systems have not been certified and accredited; (2) All organizational components' information security weaknesses are not included in a POA&M; (3) Data in the enterprise management tool, Trusted Agent FISMA, is not complete or current; (4) System contingency plans have not been developed or tested for all systems; and (5) FISMA metrics data, captured within Trusted Agent FISMA and used by the Chief Information Officer (CIO) to monitor component's security programs, is not comprehensively verified. While the Department has issued substantial guidance designed to create and maintain secure systems, we identified areas where agency wide information security procedures require strengthening: (1) certification and accreditation; (2) vulnerability testing and remediation; (3) penetration testing; (4) contingency plan development and testing; (5) incident detection, analysis, and reporting; (6) security configuration; and, (7) specialized security training.

Fiscal Year 2005 Progress:

The Chief Information Security Officer (CISO) revised the baseline information technology (IT) security policies and procedures in the Sensitive Systems Policy Publication 4300A and its companion, the Sensitive Systems Handbook 3; and National Security Systems Policy Publication 4300B and its companion, the National Security Systems Handbook 4 to include updated policy on Public Key Infrastructure (PKI), wireless communication and media reuse and disposition. Other changes included mandating that the components ensure that their systems meet the requirements specified in the Department's baseline configuration guides, as well as the acceptable methods for encrypting sensitive information. Additionally, the Department issued the Department of Homeland Security Information Security Program Plan of Action and Milestones (POA&M) Process Guide 5 which provides the department and components with the necessary guidance and procedures to develop, maintain, report, and mature the POA&M process. Together, these policies and procedures, if fully implemented by components, should provide the Department with an effective information security program that complies with FISMA requirements.

Non-Compliance with Laws and Regulationsas of September 30, 2005

Title: Federal Managers' Financial Integrity Act of 1996 (FMFIA)
Entities: USCG, EP&R, ICE, TSA
Originally Reported: FY 2004
Target Date: FY 2006

Description:

Management's FMFIA report did not contain corrective action plans for all material weaknesses identified in the PAR. The Department and its components— USCG, EP&R, ICE, and TSA — have not established effective systems, processes, policies and procedures to evaluate and report on internal accounting and administrative controls, and conformance of accounting systems to properly and accurately report on compliance with Sections FMFIA Sections 2 and Section 4.

Corrective Actions:

The Department has developed and implemented a comprehensive plan to ensure compliance with FMFIA. This includes implementing an internal control program and hierarchy Department-wide; issuing timely policy guidance on FMFIA reporting and adopting the tools to allow for the standardization of FMFIA reporting throughout the organization.

Fiscal Year 2005 Progress:

A corrective action plan directive and process guide have been drafted and will be adopted fiscal year 2006 Q1. An FMFIA process has been developed to properly and accurately report on internal control, systems security and ensure the reliability of financial reporting throughout the organization. Further guidance has been developed to assure that the Department is in compliance with the provisions of OMB Circular No. A-123.

Title: Single Audit Act Amendments of 1996, and Laws and Regulations Supporting OMB Circular No. A-50, Audit Follow-up, as revised
Entities: SLGCP, EP&R, TSA
Originally Reported: FY 2004
Target Date: FY 2006

Description:

Although certain procedures have been implemented to monitor grantees and their audit findings, it was noted that EP&R, SLGCP and TSA did not have procedures in place to fully comply with provisions in OMB Circular No. A-133 and No. A-50 that require them to timely obtain and review grantee single audit reports and follow upon questioned costs and other matters identified in these reports.

Corrective Actions:

FEMA, SLGCP, and TSA are developing and implementing the policies and procedures needed to create a viable internal control program in line with OMB and GAO standards. SLGCP is creating an Audit Resolution Team to ensure compliance with No. A-133.

Fiscal Year 2005 Progress:

FEMA and TSA have completed corrective actions to remediate this weakness but have not verified and validated the correction. SLGCP has delayed implementation of the Audit Resolution Team until the end of fiscal year 2006 Q1 due to delays in the hiring process.

Title: Improper Payments Information Act of 2002 (IPIA)
Entities: Department
Originally Reported: FY 2004
Target Date: FY 2005

Description:

The Department did not: (1) systematically review and identify all programs susceptible to significant erroneous payments; and (2) test all material programs for improper payments.

Corrective Actions:

The Department will expand IPIA program testing from each components largest material program to all material programs. Smaller programs will undergo a qualitative risk assessment to identify any exceptional circumstances. Recovery and internal control audit test work will be used to verify random sample test results.

Fiscal Year 2005 Progress:

Department components identified and performed random sample payment testing on their largest IPIA program to determine with statistical certainty whether the program was at high risk for issuing improper payments. No program was assessed as at high risk for issuing improper payments (following OMB's $10 million and 2.5% criteria). Recovery audits results at ICE and CBP were consistent with component testing.

Title: Department of Homeland Security Financial Accountability Act of 2004
Entities: Department
Originally Reported: FY 2005
Target Date: FY 2006

Description:

Section 3 states that the President of the United States shall appoint a Chief Financial Officer of the Department of Homeland Security not later than 180 days after the enactment date. Currently, the Department is not complying with Section 3 and the Department's management has not sought a waiver or amendment to the law.

Corrective Actions:

Have a Congressionally confirmed CFO appointed by the President.

Fiscal Year 2005 Progress:

Not applicable, new finding.

Title: Government Performance and Results Act of 1993
Entities: Department
Originally Reported: FY 2005
Target Date: FY 2006

Description:

The fiscal year 2006 Department of Homeland Security Annual Performance Plan does not include details related to requisite resources to meet Department goals or a description of the means used to verify and validate performance measure results. The Department has not consistently presented performance measures in the PAR as written in the annual performance plans, has not provided explanations of performance results and does not have supporting documentation substantiating the changes in performance measure goals between the annual performance plan and the PAR.

Corrective Actions:

Department management will need to ensure that requisite resource needs are clearly linked by fully described means to performance measures that are validated and verified. Annual performance plans will need to be reviewed to ensure that they contain proper performance result explanations backed by sufficient supporting documentation and that goals are consistent between the annual performance plan and the PAR.

In addition, the Budget and Accounting Procedures Act of 1950, as amended, states that "the head of each covered executive agency shall prepare and submit to the Congress and the Director of the OMB audited financial statements for the preceding fiscal year, covering all accounts and associated activities of each office, bureau, and activity of the agency."

Fiscal Year 2005 Progress:

Not applicable, new finding.

COMPLIANCE WITH LAWS AND REGULATIONS

Federal Managers' Financial Integrity Act (FMFIA)

The FMFIA requires agencies to establish and maintain internal control. Management must annually evaluate and report on the control and financial systems that protect the integrity of Federal programs; Section 2 and Section 4 respectively. The requirements of FMFIA serve as an umbrella under which other reviews, evaluations and audits should be coordinated and considered to support management's assertion about the effectiveness of internal control over operations, financial reporting, and compliance with laws and regulations. The Secretary's Assurance Statement is structured around reporting the results of management's evaluation of Section 2 and Section 4 and the other laws and regulations under its umbrella that are outlined below.

Federal Financial Management Improvement Act (FFMIA)

The FFMIA requires the Department to have financial management systems that substantially comply with the Federal financial management systems requirements, standards promulgated by the Federal Accounting Standards Advisory Board (FASAB) and the U.S. Standard General Ledger (USSGL) at the transaction level. Financial management systems must have general and application controls in place in order to support management decisions by providing timely and reliable data.

Management must make a determination annually about whether the agency's financial management systems are in substantial compliance with the FFMIA. For systems that are found not to be compliant, management will develop a remediation plan to bring those systems into substantial compliance. The agency is reporting fiscal year 2005 non-compliance in the Secretary's Assurance Statement, where it is included with Section 4 of FMFIA.

Federal Information Security Management Act (FISMA)

FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal government's information and information systems such as the development of minimum standards for agency systems.

FISMA introduces a statutory definition for information security. The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; and (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

FISMA requires each agency to perform for each system "periodic testing and evaluation of the effectiveness of information security policies, procedures and practices, to be performed with a frequency depending on risk, but no less than annually." This evaluation will include the testing of management, operational and technical controls. The results of the fiscal year 2005 Department of Homeland Security Information Security C&A Remediation Plan is summarized in the following section. Significant deficiencies found under FISMA are reported as material weaknesses under FMFIA Section 4, included in the Secretary's Assurance Statement.

Improper Payments Information Act of 2002

The Improper Payments Information Act (IPIA) of 2002 (P.L. 107-300) requires Federal agencies to carry out a cost-effective program for identifying payment errors and recovering any amounts overpaid. An improper (or erroneous) payment includes any payment that should not have been made or that was made in an incorrect amount under statutory, contractual, administrative or other legally applicable requirement. Incorrect amounts include: overpayments; underpayments (including inappropriate denials of payment or service); any payment made to an ineligible recipient or for an ineligible service; duplicate payments; payments for services not received; and payments that do not account for applicable discounts.

To comply with IPIA requirements and related guidance from OMB, the agency carried out the next phase of a plan begun in fiscal year 2004, to reduce its susceptibility to issuing improper payments. In fiscal year 2004, the agency completed a risk assessment of major programs. This risk assessment did not identify any programs as high risk for issuing improper payments. In fiscal year 2005, each component completed statistically significant testing of payments from their largest program (with the exception of EP&R, which tested its second largest program highlighted in an improper payment-related OIG finding). All major payment types within the largest program were sampled. Estimated error rates and amounts were calculated. As in fiscal year 2004, no program was found to exceed the OMB defined high-risk standards of $10 million and 2.5 percent.

In fiscal year 2005, the Department commenced recovery audit efforts at CBP and ICE that have, to date, identified more than $2.2 million in erroneous payments and recovered more than $1.8 million. Additional IPIA information can be found in Other Accompanying Information in Section III of the Performance and Accountability Report.

Government Performance and Results Act (GPRA)

To support results-oriented management, GPRA requires that the Department develop strategic plans, set performance goals, and report annually on actual performance compared to goals. These plans and goals are integrated into (i) the budget process, (ii) the operational management of agencies and programs, and (iii) accountability reporting to the public on performance results, and on the integrity, efficiency, and effectiveness with which they are achieved. Similarly, the Program Assessment Rating Tool's (PART) primary purpose is to assess program effectiveness and improve program performance. The PART has also become an integral part of the budget process when making funding resource allocations or decisions.

Performance results are reported in Section II of the PAR, and the Secretary's Assurance Statement asserts to the completeness and accuracy of performance data.

Chief Financial Officers Act, as amended (CFO Act)

The passage of the Department of Homeland Security Financial Accountability Act in fiscal year 2005 made the Department of Homeland Security a CFO Act agency. The CFO Act requires agencies to both establish and assess internal control related to financial reporting. The Act requires the preparation and audit of financial statements. In this process, auditors report on internal control and compliance with laws and regulations related to financial reporting. This Performance and Accountability Report is structured and presented to comply with the CFO Act.

Inspector General Act of 1978, as amended (IG Act)

The IG Act provides for independent reviews of agency programs and operations. The annual CFO audit of the Department's financial statements included in this report and the opinion rendered by KPMG fulfills the IG requirements under the Government Auditing Standards and OMB Bulletin No. 01-02, Audit Requirements of Federal Financial Statements, as amended. In particular, to report material weaknesses in internal control related to financial reporting and noncompliance with laws and regulations as part of the financial statement audit. Auditors also provide recommendations for correcting the material weaknesses. Management is required by the IG Act to follow up on audit recommendations and has used these reviews to identify and correct problems resulting from inadequate or poorly designed controls, and to build appropriate controls into the Department's programs.

Single Audit Act, as amended

The Single Audit Act, as amended, requires financial statement audits of non-Federal entities that receive or administer grant awards of Federal monies. The financial statement audits include testing the effectiveness of internal control and determining whether the award monies have been spent in compliance with laws and regulations. The Department provides a number of grant programs that are reflected in the Performance and Accountability Report. It is management's responsibility to review the audits of the recipients to determine whether corrective actions are implemented with respect to audit findings.

Clinger-Cohen Act of 1996

The Clinger-Cohen Act requires agencies to use a disciplined capital planning and investment control (CPIC) process to maximize the value of and assess and manage the risks of IT acquisitions. The Act requires that agencies establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public. The MD&A, Section I, and the Performance Information included in Section II reflect the Agency's compliance with the requirements of this Act.

COMPLIANCE WITH OTHER KEY LEGAL AND FINANCIAL REGULATORY REQUIREMENTS

The Department is required to comply with several other key legal and regulatory financial requirements, including the Prompt Payment Act and the Debt Collection Improvement Act.

Prompt Payment Act

The Prompt Payment Act requires Federal agencies to make timely payments (within 30 days of receipt of invoice) to vendors for supplies and services, to pay interest penalties when payments are made after the due date, and to take cash discounts only when they are economically justified. The Department's components submit Prompt Payment data as part of data gathered for the CFO Council's Measurement Tracking System (MTS). Periodic reviews are conducted by the components to identify potential problems. Interest penalties as a percentage of the dollar amount of invoices paid subject to the Prompt Payment Act has remained below 0.1 percent throughout the July 2004 – July 2005 period that the statistics have been kept (MTS statistics are reported with a two-month lag).

Debt Collection Improvement Act (DCIA)

The Department complies with the Debt Collection Improvement Act (DCIA) and its key provisions of turning over all eligible debt to the Treasury Offset Program (TOP) for collection, timely notification to the Internal Revenue Service on Form 1099C of any discharged or closed out debt, accurately reporting debt statistics in Treasury's Report on Receivables (TROR) system, certifying and explaining any discrepancies between TROR and debt-related standard general ledger account balances, aggressively servicing and collecting delinquent debts, and denying direct and indirect loans to delinquent debtors. The Department also complies with a Debt Collection Improvement Act annual reporting requirement to OMB. The Department supported a 180-day moratorium on the collection of debts in the Gulf Coast region that the Treasury Department offered to all Federal agencies in the aftermath of Hurricane Katrina.

Biennial Review of Fees

The CFO Act of 1990 requires biennial reviews by Federal agencies of agency fees, rents, and other charges imposed for services and things of value provided to specific beneficiaries, as opposed to the American public in general. The objective of these reviews is to identify such activities and begin charging fees, if permitted by law, and to periodically adjust existing fees to reflect current costs or market value. These updated fees minimize the general taxpayer subsidy of specialized services or things of value (such as rights or privileges) provided directly to identifiable non-Federal beneficiaries. The Department did not become subject to the CFO Act of 1990 provisions until fiscal year 2005 (with the passage of the Department of Homeland Security Financial Accountability Act). The Department did not conduct a biennial review of its user fee programs during fiscal year 2005.

MANAGEMENT PLANS

Department of Homeland Security Information Security C&A Remediation Plan (FISMA)

The House Appropriations Committee (HAC) Report 109-079, Department of Homeland Security 2006 Appropriations Bill, directed the "Department's CIO to develop a plan to address the weaknesses in DHS' information security" by October 1, 2005. In addition, the Office of the Inspector General (OIG) was directed to review the plan and report back to the committee by the end of November 2005. The committee report identified four weaknesses in the information security program. The Department has completed actions to fully address one of the weaknesses - the lack of a complete and accurate inventory.

The Department of Homeland Security Certification and Accreditation (C&A) Remediation Plan outlines how the Department will meet its goal of 100 percent C&A of all IT systems by the end of fiscal year 2006. The objective of the plan is to provide agency-wide information security procedures to report on the progress of the C&A efforts within the Department. In addition, this plan explicitly addresses the three remaining weaknesses identified in the HAC Report.

The Department's C&A Tool will be used to complete all C&As. The C&A Tool imposes a standardized process and will result in FISMA-compliant products. Testing of contingency plans is incorporated into the Department's C&A process. Contractor systems are included in the comprehensive inventory completed in fiscal year 2005.The plan uses the processes and Federal Information Security Management Act (FISMA) reporting and C&A tools implemented by the Office of the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) in fiscal year 2005. The remediation plan outlines how the components will not only be able to identify the C&A activities and documentation that they are required to complete, but also how C&A remediation scores will be calculated and measured at the departmental-level.

REMEDIATION PLAN SUMMARY

	Remediation Deliverables	Weights	Cum.
1	FIPS 199 Categorization Completed	5%	5%
2	Privacy Impact Determination/Assessment	3%	8%
3	E-Authentication Determination/Assessment	2%	10%
4	Risk Assessment	10%	20%
5	System Security Plan	20%	40%
6	Contingency Plan	10%	50%
7	Contingency Plan Test Results	5%	55%
8	Security Test & Evaluation Plan	10%	65%
9	Security Assessment Report	15%	80%
10	ATO Letter	10%	90%
11	Annual Self Assessment	10%	100%

This remediation plan applies an earned-value management approach by identifying 11 C&A artifacts that must be completed for every Department IT system. The above table summarizes the deliverables and the weightings to be assigned to the deliverables that will be used to develop the C&A remediation score.

Credit will only be given for artifacts (e.g., Privacy Impact Assessment [PIA], and System Security Plan [SSP]) if the actual artifact is uploaded into TrustedAgent FISMA (TAF), the Department's FISMA reporting tool. Visibility of all artifacts at the Department level, while also ensuring that artifacts are fully aligned with the inventory, is critical to the Department's ability to track progress during the next year.

Each component must establish objectives and milestones, and closely monitor progress to ensure success. Each component CIO was required to submit a fiscal year 2006 Remediation Plan to the Department's CISO during October 2005. In addition, a POA&M must be developed for all unaccredited systems and entered into the FISMA reporting tool.

The Department established the following interim performances objectives to ensure progress.

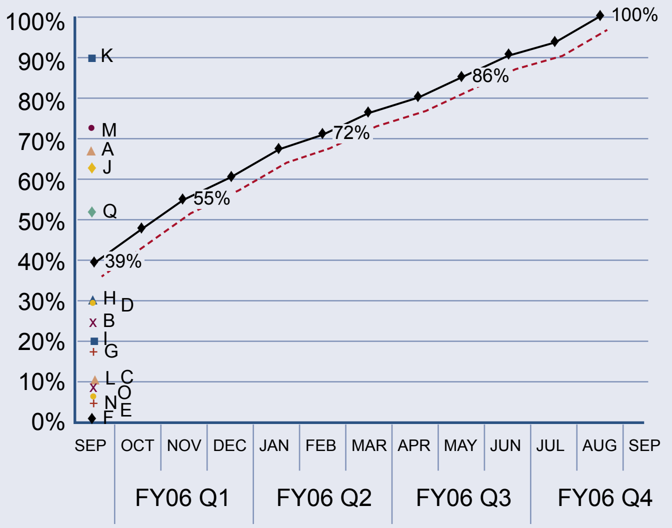
PERFORMANCE OBJECTIVES

FY 2006 Quarter	C&A Completion Objective
Ending Qtr 1	55%
Ending Qtr 2	72%
Ending Qtr 3	86%
Ending Qtr 4	100%

ACCOUNTABILITY

A detailed remediation status report by component will be delivered monthly to the component CIO and Information System Security Manager (ISSM). Status reports highlight the overall progress against departmental and component objectives for the remediation effort. At a minimum, the status reports will consist of the sample diagrams below.

REMEDIATION PROGRESS BY COMPONENT



DHS MONTH X PERFORMANCE

Component	Systems	Goal	Actual	Gap	Trend
A	40	39%	68%	29%	
B	100	39%	24%	15%	
C	5	39%	10%	29%	
D	70	39%	35%	-4%	
E	10	39%	4%	-35%	
F	1	39%	0%	-39%	
G	30	39%	16%	-23%	
H	130	39%	35%	-4%	
I	20	39%	18%	-21%	
J	10	39%	63%	24%	
K	5	39%	90%	51%	
L	10	39%	10%	-29%	
M	10	39%	73%	34%	
N	70	39%	5%	-34%	
O	200	39%	7%	-32%	
P	40	39%	6%	-33%	
Q	15	39%	51%	12%	
DHS Overall	**766**	**39%**	**23%**	**-16%**	

🟦 Greater than or equal to +5% of Performance

🟩 Within +5% of Performance goal

🟨 Within -5% of Performance goal

🟥 Less than or equal to -5% of Performance

SUMMARY

The Department submitted the required information security C&A remediation plan to the OIG on September 30, 2005, to address the three remaining weaknesses outlined in the House Appropriations Committee Report 109-079. The approach detailed in this remediation plan, if implemented and centrally managed, will result in an improved security posture for the Department in fiscal year 2006, one that has all its systems accredited. To continue to improve the security posture, the fiscal year 2007 strategy will be to improve performance, resolve security deficiencies, and perform more independent verification to identify vulnerabilities and weaknesses associated with the component's security practices.

FINANCIAL MANAGEMENT SYSTEMS FRAMEWORK

Department-wide Initiatives: In August 2003, the Department initiated plans to provide solutions for its financial management needs by establishing the Resource Management Transformation Office (RMTO) under the Office of the CFO. The RMTO initiated the financial enterprise solution project known as "Electronically Managing Enterprise Resources for Government Effectiveness and Efficiency" (eMerge2). The eMerge2 program sets the strategic direction for migration, modernization and integration of departmental financial, accounting, procurement, grants, asset management, and travel systems. In fiscal year 2005, with the vision and requirements of the program firmly established, the program began experiencing difficulties in the integration of the system components. The Department took a strategic pause in the program to evaluate solution options: 1) outsourcing the solution to the private sector, 2) outsourcing to one of the recently established government Centers of Excellence (COE) or 3) revisiting current financial service providers within the Department while still exploring the feasibility of building the Commercial Off-The-Shelf (COTS) integrated solution.

The Office of the CFO has adopted an approach to the enterprise solution that will focus on three phases:

- Consolidate systems/service providers and address material weaknesses;
- Implement corporate unifying features (integration capabilities); and
- Optimize environment to achieve efficiencies and effectiveness.

While the methodology for achieving the eMerge2 vision has changed, the Department's financial management vision and requirements remain unchanged.

CBP: In October 2004, CBP implemented the last of three major releases of SAP, an Enterprise Resource Planning (ERP) system. SAP replaced numerous legacy financial, procurement and property systems with a single fully integrated solution. This system gives CBP a state-of-the-art, fully integrated system in which to plan, acquire, track and fully account for all purchases and assets as well as track budgets and provide management with timely and accurate financial reports. The post-SAP implementation period has proved challenging for CBP. Reorganizations among the Department's elements that continue to expand our size and structure, as well as a continuous desire to add to or improve upon this new functionality, have thwarted efforts to focus on stabilization of the SAP system. SAP brings forth an entirely new technology and operating environment. Business processes have been changed or eliminated to add value to the investment and CBP itself. SAP processes transactions and provides reporting capability in less time than previously performed by 11 legacy applications. All reorganizations have been accomplished without issue, and SAP users have received training to enable them to adapt their processes to match the benefits of the system.

The future holds many prospects for expanding and improving the SAP system at CBP. Several legacy asset management-related systems still exist within CBP's enterprise architecture. Many of these are good candidates for integration into SAP and will be replaced. New systems being planned for and developed will need to be interfaced including the CBP future eTravel system and the many solutions sure to be born out of the eMerge2 effort. These plans cannot exclude continued efforts to build on the momentum the Customs Modernization Office has created in developing SAP as a core system for the Automated Customs Environment (ACE). Many successes have been realized by the implementation of SAP at CBP, and it is plain to see that there are many more tasks to be accomplished. All of these tasks will be completed as efficiently and timely as they have in the past in order to continue to enable the CBP frontline to accomplish their goals of fighting terrorism and safeguarding the American homeland.

FLETC: In May 2005, FLETC implemented e-Travel and became the first component within the Department to use FedTraveler.com, a web-based end-to-end online system of processing and booking of temporary duty (TDY) travel. During the early stages of the e-Travel implementation, FLETC identified more than 150 system issues and software glitches related to document processing, online booking of airline and hotel reservations, customer support, etc. Coordinating aggressively with the contractor to resolve the issues, FLETC re-engineered its TDY travel business processes and progressively took advantage of the e-Travel automated processing features. During fiscal year 2005, approximately 2,000 Travel Plans and Expense Reports for FLETC staff were processed through FedTraveler.com.

FLETC uses the Momentum Financial System for its financial management services. This system has served FLETC well over the past five years, contributing to three consecutive unqualified opinions prior to the transfer to the Department of Homeland Security and continued clean annual financial audits. While the current Momentum financial management software is adequate, FLETC is looking to fully take advantage of advances in technology and upgrade its five-year-old integrated core financial management software. FLETC is considering all financial management software options and is seeking the optimum solution for all FLETC and Department of Homeland Security financial management requirements.

FLETC also upgraded its Electronic Certification System for automated disbursement schedules transmitted to the servicing Department of Treasury finance center to the Financial Management System SPS in August 2005. Besides being Section 508-compliant, the SPS incorporates PKI, a secure means of transmitting data through the Internet through the use of a public and private cryptographic key pairing.   Because of the SPS thin-client application that allows easy file transfer, FLETC can now confirm disbursing schedules within one day and promptly post the payment data in the financial management system, which enhances fund balance reconciliation and customer service on payment queries.

U.S. Secret Service: In October 2004, the USSS implemented a new Joint Financial Management Improvement Program (JFMIP) certified core financial management system, Oracle Federal Financials, as well as new administrative systems to support property management (Sunflower Asset Management), procurement management (Compusearch PRISM) and inventory management (Oracle Inventory). The software solution implemented includes integration between the new software components, as well as interfaces with other internal and external administrative systems (Master Personnel System, Gelco Travel Manager, NFC Payroll, Gelco Third Party Draft, Purchase Card Provider). In addition, the solution also includes extensions to support unique business processes at USSS, such as imprest/confidential fund accountability and replenishment business processes. This major implementation effort was completed in approximately 3 1/2 years, which included the requirements definition phase, software selection phase, systems integrator selection phase, and software configuration/development and implementation phase. Implementation efforts of this complexity and magnitude at Federal agencies often take a much longer period of time to complete, and in some instances, the projects are cancelled after several years of effort.

Fiscal year 2005 was successfully closed in mid-October 2005, which marked the anniversary of implementing the new financial management system. The first year of using the new system brought several challenges due to the business process changes and the large number of users in the field entering financial transactions. In addition, the system was implemented during a time at USSS when there was an unusually large volume of financial transactions that needed to be recorded in the new system (e.g., hotel invoices related to 2004 presidential campaign activities). Several enhancements were implemented during the year, including custom front-end screens to provide a more user-friendly mechanism for the field users to record financial transactions. Additional enhancements are planned this year, particularly in the areas of analyzing and reconciling financial transactions and providing reports to the offices to manage allocations.

Coast Guard: At the beginning of fiscal year 2005, the USCG began cross-servicing TSA and FAMS on the USCG Core Accounting System (CAS). CAS is: seven modules of the Oracle Financials (core accounting functionality); FPD (the simplified acquisition tool); Contract Information Management System (CIMS), CompuSearch PRISM (product for management of large contracts); Sunflower (property management) and Markview (170 Systems for invoice imaging). USCG also provided TSA the ability to perform automated agency-wide physical inventory of all its property. This functionality is fully integrated with Sunflower.

The USCG continued its roll-out of additional real-time integration between system components. This integration uses a Service Oriented Architecture approach using web services in real time. In addition, the USCG introduced the capability for accrual-based accounting into the core accounting system. This capability was implemented using a web-based receipts module, which TSA now uses. USCG also introduced the ability to apply multiple accounting lines to a single line item in FPD. FPD To Go, the disconnected environment version of FPD, was deployed to nine cutters throughout the fiscal year. CIMS was fully deployed to the Pacific Area. Furthermore, USCG began the initiative to move to LINUX-based hardware architecture. In August 2005, USCG successfully transitioned USCG, TSA and FAMS payroll processing function from the Department of Transportation (DOT) to the U.S. Department of Agriculture's National Finance Center (NFC). This integration ensures that payroll costs are accurately accounted for in the general ledger.

In 2006, USCG will continue with its migration to a LINUX-based hardware architecture and Real Applications Cluster (RAC) technology. USCG has begun the e-Travel initiative to move USCG, TSA and FAMS to a centralized travel system and have it integrated in real time with CAS. USCG also selected and procured a centralized reporting tool (Informatica) to be rolled out throughout fiscal year 2006. Additionally, USCG will continue with its FPD To Go and CIMS migrations. Inclusive of this effort is migrating Deepwater to both CIMS and FPD. USCG will continue to look at moving to a single system process for USCG, TSA and FAMS and eliminating general ledgers outside of the core accounting system.

TSA: At the beginning of fiscal year 2005, TSA migrated its financial management operations from the DOT financial systems environment to the USCG financial systems environment. USCG's suite of financial systems includes the Core Accounting System (Oracle Federal Financials 11.5.9), the Finance and Procurement Desktop (a front-end tool that enables program and field office personnel to execute requisitions and track spending online), the Markview invoice imaging and routing system, and the Sunflower Asset Management System. At the same time, TSA migrated its outsourced accounting operations (payment and collection processing) from DOT's Finance Center to the USCG Finance Center in Chesapeake, Virginia. The migration has reduced the Department's dependency on an external department, brought the financial management activities of two of the Department's largest components under one roof, and is expected to generate economies of scale as both TSA and USCG will realize benefits from future investments in system upgrades.

Following on the successful financial systems transition, TSA migrated its payroll processing function from DOT to the NFC systems in August 2005. This transition will put TSA on the same payroll platform as all other departmental components and will result in more efficient payroll services for TSA employees. An interface from NFC to the Core Accounting System has been developed, tested and implemented to ensure that payroll costs are accurately accounted for in the general ledger.

TSA's efforts to improve financial management and systems will continue in fiscal year 2006. Early in the fiscal year, an automated contract-writing system will be deployed to replace the current manual contract writing process. In addition to easing the administrative burden of developing government contracts, the system will interface with the Core Accounting System to liquidate commitments and post obligations; processes that currently require manual data entry. Later in fiscal year 2006, TSA will begin its efforts to migrate from its legacy travel management system to the Department's eTravel solution. eTravel will allow TSA travelers to make reservations, request authorization, and submit subsequent travel vouchers from a single online system.

ICE: In order to offload the heavy reporting volume from the Federal Financial Management System (FFMS) ICE production database and to provide end users with a faster turn around time in obtaining requested reports, ICE created an FFMS reporting database that is a mirror image of the ICE production database. The data is updated every two hours. The reporting database is used primarily to run existing FFMS reports. Users have reported excellent response times and extreme confidence in the accuracy of the reporting data. This database enables program managers to obtain necessary financial information in a timely manner and in a user friendly format through enhanced reporting capabilities. Transferring the bulk of reporting to the reporting database allowed transaction processing to continue in the production database unheeded. Both reporting and transactional processing were greatly improved over the previous end of year.

In October 2004, ICE implemented PRISM, the Department's procurement system of choice. PRISM minimizes data entry and maximizes process efficiency through electronic routing and workload management. Since its implementation, ICE has recognized the advantage of having an electronic interface between PRISM and the FFMS. An interface will significantly improve ICE's financial management capabilities by eliminating the manual reconciliation of financial data in both systems. Additionally, it will automate the input of financial information and eliminate the double entry of financial data into both systems. ICE is moving forward to develop and implement the interface in fiscal year 2006. Once in place, ICE can eliminate the commitment accounting reconciliation process and also directly obligate procurement actions when appropriate. The implementation of the PRISM/FFMS interface is eagerly anticipated and represents a major milestone in ICE's efforts to streamline and automate its business processes and improve overall financial management.

Analysis of Financial Statements

These financial statements are prepared in accordance with established Federal accounting standards and are audited by the independent accounting firm of KPMG LLP. It is the Department's goal to improve financial management and to provide accurate and reliable information that is useful for assessing performance and allocating resources.

Figure 1 illustrates a condensed version of the Department's Consolidated Balance Sheet.

Condensed Consolidated Balance Sheet
As of September 30, 2005 and 2004
(In Millions)

ASSETS	**FY 2005**	**FY 2004**	**Change**
Intragovernmental Assets	101,040	38,428	$62,612
Tax, Duties and Trade Receivables, Net	1,400	1,273	127
General Property, Plant and Equipment, Net	10,470	9,746	724
Other	1,596	1,359	237
Total Assets	**114,506**	**50,806**	**63,700**
LIABILITIES			
Intragovernmental Liabilities	3,158	2,731	427
Claims and Claims settlement Liabilities	23,433	1,417	22,016
Accrued Payroll and Benefits	2,845	2,692	153
Military Service and Other Retirement Benefits	29,021	26,502	2,519
Other	11,288	8,977	2,311
Total Liabilities (Note 12)	**69,745**	**42,319**	**27,426**
Net Position			
Unexpended Appropriations	87,166	25,504	61,662
Cumulative Results of Operations	(42,405)	(17,017)	(25,388)
Total Net Position	**44,761**	**8,487**	**36,274**
Total Liabilities and Net Position	**114,506**	**50,806**	**63,700**

ASSETS

In fiscal year 2005, the Department's assets totaled $114,506 million. This is an increase of $63,700 million over the prior year's assets totaling $50,806 million. Intragovernmental Assets are primarily the Fund Balance with Treasury and Advances and Prepayments. Intragovernmental Assets and General Property, Plant, and Equipment comprise 97 percent of total assets. The largest increase to assets relates appropriations for Gulf Coast hurricane disaster relief funding. ***Figure 2*** summarizes the Department's assets as of September 30, 2005 and September 30, 2004.

The increase in Intragovernmental Assets is primarily due to an increase in the Fund Balance with Treasury from Appropriated Funds that represents $97,004 or 96 percent of the total, A portion of the Fund Balance with Treasury also includes Trust Funds, used to hold receipts for specific purposes; Revolving Funds, Liquidating and Working Capital Funds, used for continuing cycles of business-like activity; Special Funds, earmarked for specific purposes and Deposit Funds, amounts received as advances for which final disposition has not been determined. General Property, Plant and Equipment are primarily composed of aircraft, vessels, vehicles, land, structures, facilities, leasehold improvements, software, information technology, and other equipment that are used for general operations. Multi-use heritage assets consist primarily of buildings and structures owned by CBP and USCG.

FIGURE 2 - ASSETS

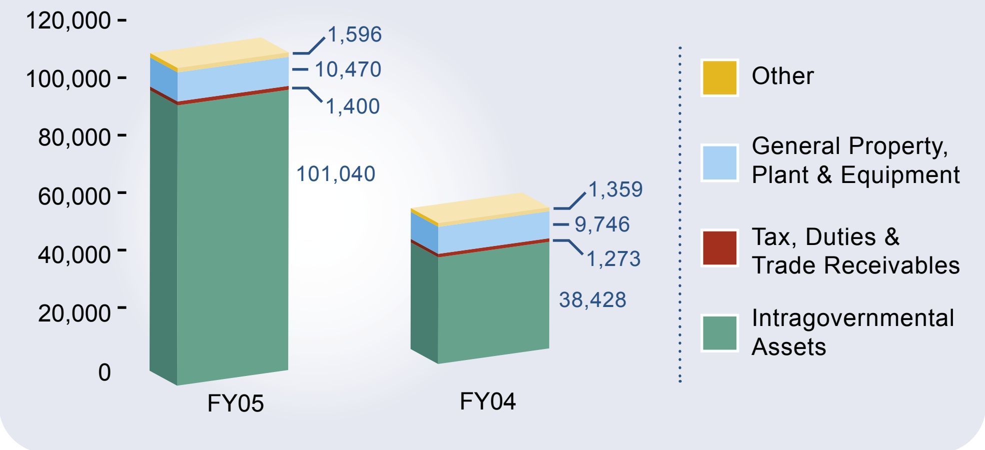
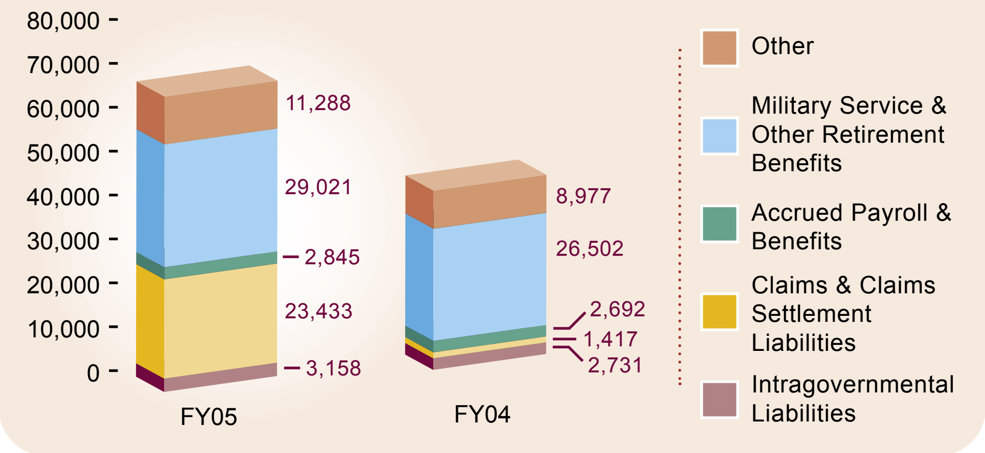


FIGURE 3 - LIABILITIES



LIABILITIES

In fiscal year 2005, the Department's liabilities totaled $69,745 million. This is an increase of $27,426 million over the prior year's liabilities, which totaled $42,319 million. Intragovernmental Liabilities is primarily debt to the U.S. Treasury and advances and deferred revenue.

Claims and Claims Settlement Liabilities (related to the National Flood Insurance Program claims) and Military Service and Other Retirement Benefits (arising from USCG personnel benefits) comprise 75 percent of the Department's total liabilities. Figure 3 summarizes the Department's liabilities as of September 30, 2005, and September 30, 2004.

Federal agencies by law cannot disburse money unless Congress has appropriated funds. Funded liabilities are expected to be paid from funds currently available to the Department. The Department's unfunded liabilities consist primarily of environmental and legal contingent liabilities and unfunded employee compensation costs, including FECA and annual leave. These liabilities will be paid from funds made available to the Department in future years. The associated expense is recognized in the period in which the liability is established, regardless of budgetary funding considerations.

ENDING NET POSITION

The Department's net position at the end of fiscal year 2005, disclosed in the Consolidated Balance Sheet and the Consolidated Statement of Changes in Net Position was $44,761 million, an increase of about $36,274 million from the previous year.

The net position of the Department consists of two components (1) Unexpended Appropriations of $87,166 million and (2) Cumulative Results of Opera¬tions of ($42,405) million. The growth in Unexpended Appropriations is primarily attributable to the increase in unexpended appropriations for Gulf Coast hurricane relief.

RESULTS OF OPERATIONS

The Department's net cost of operations for fiscal year 2005 was $66,405 million. This is an increase of $33,277 million from the previous year's net cost of $33,128 million. Most increase costs incurred by the Department for fiscal year 2005 are directly related to EP&R (FEMA) disaster relief efforts. The Department of Homeland Security Strategic Plan outlines the follow¬ing mission goals: Awareness, Prevention, Protection, Response, Recovery, Service and Organizational Excellence. EP&R (FEMA) Costs by Strategic Goals (Protection, Response and Recovery) represent 57 percent of the Department's total net cost of operations.

Figure 4 illustrates a condensed version of the Department's Statement of Net Cost.

Condensed Consolidated Statement of Net Costs
For the Years Ended September 30, 2005 and 2004
(In Millions)

	2005	2,004	Change
Cost by Directorate and Component			
Border Transportation Security	14,367	13,741	626
Emergency Preparedness and Response	37,627	5,988	31,639
Information Analysis and Infrastructure Protection	652	497	155
Science and Technology	731	755	(24)
United States Coast Guard	9,369	8,160	1,209
United States Secret Service	1,483	1,368	115
United States Citizenship and Immigration Services	-331	448	(779)
Departmental Operations and Others	2,507	2,171	336
Net Cost of Operations	66,405	33,128	33,277
Total Cost	74,018	39,448	34,570
Cost of Transferred Operation	0	98	(98)
Total Revenue	7,613	6,418	1,195
Net Cost of Operations	66,405	33,128	33,277

REVENUES

During fiscal year 2005, the Department earned approximately $7,613 million in revenues; this is an increase of about $1,195 million from September 30, 2004. The increase in revenue is due primarily to an increase in exchange revenue by BTS.

The Department classifies revenues as either exchange or non-exchange revenue. Exchange revenues are those that derive from transactions in which both the government and the other party receive value, and that are directly related to departmental operations. The Department also collects non-exchange duties taxes and fee revenues on behalf of the Federal government. These are presented in the Statement of Custodial Activity rather than the Statement of Net Cost.

Examples of non-exchange revenues are monies that the Federal govern¬ment collects as a result of its sovereign powers rather than as a result of providing goods or service for a fee. Donations to the Department are also reported as non-exchange revenues. Non-exchange revenues earned are either retained by the Department to further its mission or returned to the General Fund of the Treasury.

CUSTODIAL ACTIVITY

In accordance with Federal accounting standards, revenues are presented in the Department's Statement of Custodial Activity since the collections are considered to be revenue of the Federal government as a whole rather than the Department. Revenues were $27,580 and $24,449 million as of September 30, 2005 and 2004, respectively, and include duties, user fees and excise taxes.

BUDGETARY RESOURCES

The Department receives most of its funding from general government funds administered by the U.S. Treasury and appropriated for the Department's use by Congress. These resources consist of the balance at the beginning of the year, appropriations received during the year, and spending authority from offsetting collections as well as other sources of budgetary resources (Figure 5).

The Combined Statement of Budgetary Resources provides information on the budgetary resources that were made available to the Department for the year and the status of those resources at the end of the fiscal year. Obligations of $68,621 and $45,487 million were incurred as of September 30, 2005 and 2004 on total budgetary resources of $125,680 and $53,879 million, respectively (Figure 6). The Combined Statement of Budgetary Resources is presented on a combined basis rather than a consolidated basis for consistency with budget execution information and to properly report obligations incurred by the entire Department.

FIGURE 5 – TOTAL BUDGETARY RESOURCES

(in millions)

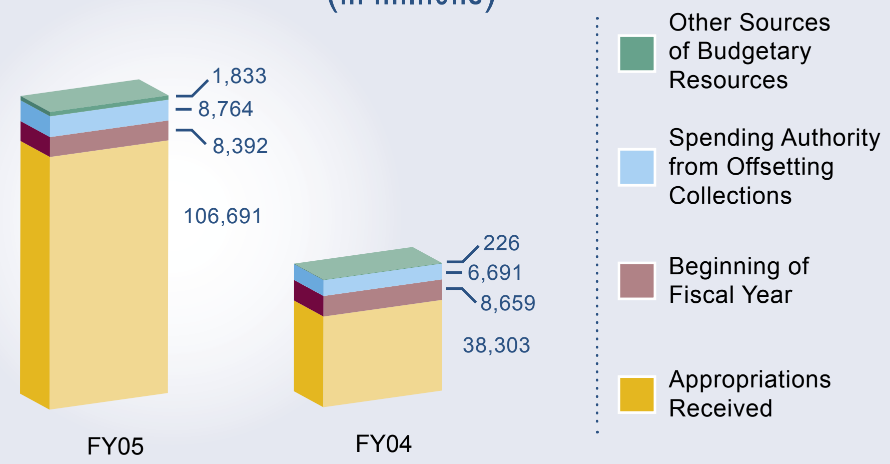
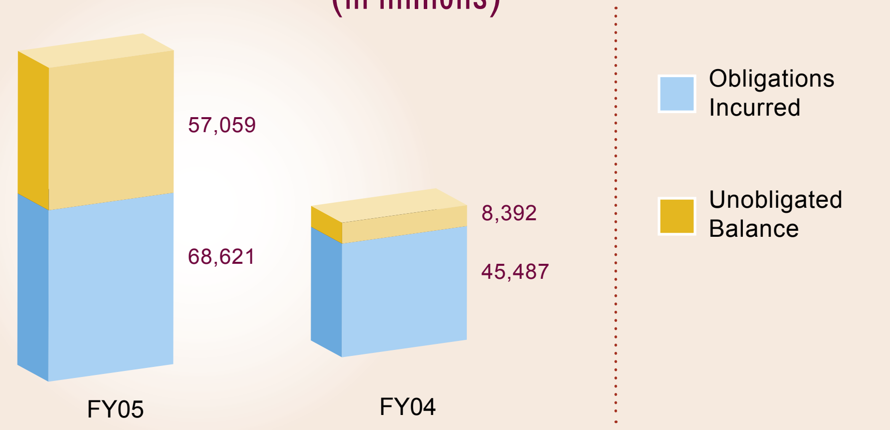


FIGURE 6 – STATUS OF TOTAL BUDGETARY RESOURCES

(in millions)



Office of Inspector General

U.S. Department of Homeland
Security
Washington, DC 20528

Homeland
Security

October 25, 2005

MAJOR MANAGEMENT CHALLENGES FACING THE DEPARTMENT OF HOMELAND SECURITY

Since its inception in March 2003, the Department of Homeland Security (DHS) worked to accomplish the largest reorganization of the federal government in more than half a century. This task, creating the third largest Cabinet agency with the critical, core mission of protecting the country against another terrorist attack, has presented many challenges to the Department's managers and employees. While DHS has made progress, it still has much to do to establish a cohesive, efficient, and effective organization.

We identified "major management challenges" facing the Department, as discussed below. These challenges are a major factor in setting our priorities for audits, inspections, and evaluations of DHS programs and operations. As required by the Reports Consolidation Act of 2000, we update our assessment of management challenges annually.

DISASTER RESPONSE AND RECOVERY

On August 29, 2005, Hurricane Katrina hit the Gulf Coast states of Louisiana, Mississippi, Alabama, and Florida, causing catastrophic damage to the region. By September 9, 2005, the Congress had passed legislation that provided $63 billion for disaster relief, the bulk of which went to the Federal Emergency Management Agency (FEMA). FEMA, in turn, tasked other federal departments and agencies through Mission Assignments and grants to affected states to assist with recovery efforts. Initial FEMA mission assignments totaled about $7 billion, over $6 billion of which went to the Department of Defense (DOD) and the Army Corps of Engineers; and FEMA grants to affected states totaled about $1 billion. In addition, some departments and agencies, including DOD, received direct appropriations for Hurricane Katrina activities. On September 24, 2005, Hurricane Rita brought further destruction to the Gulf Coast states of Louisiana and Texas. This further compounded FEMA's already overburdened resources and infrastructure. Some estimate that the total federal response and recovery cost could reach $200 billion and more.

Based on our work related to prior emergency response efforts, we have raised concerns regarding weaknesses in FEMA information systems, the flood map modernization program, contract management, grants management, and the individual assistance program. When one considers that FEMA's programs are largely administered through grants and contracts, the circumstances created by Hurricanes Katrina and Rita provides an unprecedented opportunity for fraud, waste, and abuse.

While DHS is taking several steps to manage and control spending under Katrina, the sheer size of the response and recovery efforts will create an unprecedented need for oversight. We are overseeing the funds being spent directly by DHS components, and the OIGs of 12 other departments and agencies are overseeing their respective agencies' expenditures related to Katrina, which account for about 99 percent of the funds obligated to date for FEMA disaster response and recovery efforts. During the current response phase, the primary focus of the OIGs is on contracts, particularly those awarded with no or limited competition. In addition, we are conducting an evaluation to determine the overall adequacy of DHS' emergency management program for major natural disasters, i.e., how well FEMA carried out its disaster management responsibilities in response to Hurricanes Katrina and Rita.

Further, FEMA could benefit from improving the information technology systems it uses to both mitigate risk and respond to emergency incidents. For example, floods are among the most frequent and costly of all natural disasters and have great impact in terms of economic and human losses each year. FEMA has embarked on a six-year, $1.475 billion flood map modernization program to digitize flood maps used to identify flood zones and determine insurance requirements. The current maps are paper-based, outdated, inaccurate, and inadequate. Although FEMA is making progress in the program, its Multi-Year Flood Hazard Plan does not effectively address user and funding needs, and current policies, agreements, and information sharing mechanisms do not effectively support coordination and cooperation among mapping stakeholders.

CONSOLIDATING THE DEPARTMENT'S COMPONENTS

Integrating its many separate components in a single, effective, efficient, and economical Department remains one of DHS' biggest challenges. DHS has made notable progress in this area. For example, DHS established an Operational Integration Staff to assist Departmental leadership with the integration of certain DHS missions, operational activities, and programs at the headquarters level and throughout the DHS regional structure. Further, in 2005, the Secretary initiated an internal top-to-bottom review of the Department, referred to as the Second Stage Review (2SR). The review resulted in changes to DHS organization structure. Those changes resulted in a DHS that was re-focused on risk and consequence management and further involved with its partners in other Federal agencies, state and local governments, and private sector organizations. However, much remains to be done.

For example, we reviewed and reported on a proposal to merge the Customs and Border Protection and Immigration and Customs Enforcement components within DHS. Our report, which will be issued shortly, identifies a number of significant concerns that need to be addressed, with or without a merger. In addition, as reported herein and in previous Management Challenges reports, we continue to have concerns about the Department's "dual accountability" structure for managing its business functions, particularly as related to the Chief Information Officer, Chief Financial Officer, and Chief Procurement Officer.

CONTRACT MANAGEMENT

DHS procured approximately $9.8 billion in goods and services during FY 2004 through the award of contracts, modifications, delivery orders, interagency agreements, and purchase card transactions. During the course of FY 2005 exclusive of Hurricane Katrina procurement actions, we identified a number of issues related to the challenge of building an effective contract and acquisition management infrastructure for this level of procurement activity. Those issues included the following:

- DHS needs to ensure adherence to required standards of conduct, i.e., the avoidance of improper business practices and conflicts of interest. While DHS' close relationship with the private sector may yield benefits for DHS, it also increases the potential for conflicts of interest. As noted above, we will be reviewing all Katrina related contracts awarded without competition.

- While some DHS organizational components have reported establishing program management processes within their components, currently no DHS organization is responsible for establishing Department-wide policies and procedures for program management operations. This function is critical, given the numerous, complex, mission-critical programs underway that are managed by DHS components. In May 2004, DHS instituted a program management certification process which requires increasing levels of program management certification (Levels I – III) based on varying levels of training and experience. However, some DHS organizational components still report a shortage of certified program managers to manage the Department's 110 major programs.

- DHS needs to institute several improvements to their Investment Review Board (IRB) process. For example, the DHS IRB process lacks detailed Departmental reviews, which provide decision makers with advice from functional experts, such as operational test evaluators and independent cost estimators. Also, the DHS IRB process emphasizes approval and scoring of a specific program plan, rather than selection from various alternatives.

- DHS has substantial staffing disparities in its procurement offices as the amount of awards per DHS procurement staff person ranges from a low of about $3 million up to $30 million per DHS procurement organization. In addition, some DHS procurement offices may be significantly understaffed, based on two separate studies sponsored by the Office of the Chief Procurement Officer (OCPO).

- DHS needs to establish an effective, independent oversight program. Currently there is no DHS management directive addressing OCPO oversight of DHS procurements. As a result, OCPO has limited authority to ensure compliance with DHS procurement policies and procedures. Establishing effective OCPO oversight could help DHS ensure adherence to standards of conduct, improve agency operations and ensure compliance with agency policies and procedures.

- Finally, several DHS components have large, complex, high-cost procurement programs under way that need to be closely managed. For example, CBP's Automated Commercial Environment (ACE) project will cost $3.3 billion, and the Coast Guard's Deepwater Capability Replacement Project will cost $19-24 billion and will take twenty to twenty five years to complete. Further, the Department recently awarded a $10 billion contract for the development of a system to support the United States Visitor and Immigrant Status Indication Technology (US-VISIT) program for tracking and controlling the entry and exit of all aliens entering and leaving the country through air, land, and sea ports of entry. DHS OIG will be reviewing these major procurements on an ongoing basis.

GRANTS MANAGEMENT

DHS manages a variety of disaster and non-disaster grant programs. Disaster grant awards will be substantially more than usual with the over $60 billion appropriated in late FY 2005 for disaster response and recovery efforts related to Hurricane Katrina. Also in FY 2005, DHS expected to award approximately $4.6 billion of non-disaster grants.

We are currently conducting audits of individual states' management of first responder grants and analyzing the effectiveness of DHS' system for collecting data on state and local governments' risk, vulnerability, and needs assessments. We will continue its audits of state and local governments' management of first responder grant funds and the Department's disaster relief programs, with special emphasis on Hurricane Katrina disaster response and recovery grant spending.

DHS needs to ensure that, to the maximum extent possible, homeland security assistance goes to those areas that represent the highest risks or vulnerabilities. For example, in our report on the DHS Port Security Grant program, the we reported that DHS grant making for this sector of national infrastructure was not well coordinated with the Information Analysis and Infrastructure Protection Directorate's (IAIP) Office of Infrastructure Protection, did not account for infrastructure protection priorities in the application review process, and resulted in funding of projects with low scores in the review process. Also, the DHS did not have a strong grant evaluation process in place by which to address post-award administration issues, including measuring progress in accomplishing DHS' grant objectives. Department officials noted that the Office of State and Local Government Coordination and Preparedness (SLGCP), the United States Coast Guard, the Department of Transportation's Maritime Administration (MARAD), and TSA are partners in the Request for Application development as well as the evaluation panels for the Port Security Grant Program, and that in FY 2005, SLGCP would involve IAIP's Office of Infrastructure Protection appropriately in the Port Security Grant Program. Department officials also said that in FY 2005, SLGCP plans to increase staff to allow for site visits and improved oversight of grant-funded projects.

FINANCIAL MANAGEMENT

DHS continues to face significant financial reporting problems, as evidenced by the FY 2004 and projected FY 2005 disclaimer of opinion on its consolidated financial statements. As of this date, we expect that continuing financial reporting deficiencies at ICE and Coast Guard will be the primary reasons for a FY 2005 disclaimer.

In FY 2005, ICE continues to struggle with financial management and reporting problems previously reported. In FY 2004, the financial statement auditors reported that ICE had fallen seriously behind in basic accounting functions, such as account reconciliations, analysis of material abnormal balances, and proper budgetary accounting. They reported that weaknesses in controls might have allowed ICE to violate the Anti-Deficiency Act or prevented management from knowing if they were in violation;

however the auditors were unable to complete their procedures because ICE had not adequately maintained its accounting records. With respect to Coast Guard, we expect that issues related to its military pension liability; property, plant, and equipment; and operating materials and supplies will also contribute to a disclaimer of opinion.

DHS Financial Accountability Act

Under the DHS Financial Accountability Act, DHS must undergo an audit of internal controls over financial reporting beginning in FY 2006. To "pass" such an audit, DHS and its bureaus will have to document its identification, evaluation, and testing of relevant financial controls and implement corrective actions. DHS has taken several positive steps, including the formation of a working committee to address the requirements of the law. Notwithstanding DHS' commitment to fully comply with the law, this is a significant task and will require a sustained effort not only by the Office of the CFO, but by all managers throughout the Department. We will audit the Department's FY 2006 internal control attestation during our audit of the Department's FY 2006 financial statements.

HUMAN CAPITAL MANAGEMENT

The Homeland Security Act gave DHS special authorization to design a human capital management system that fits its unique missions. In June 2004, the Department awarded a contract for services related to the development and implementation of its new human capital management system, MAXHR, and in January 2005, the Department announced its final MAXHR regulations.

Although the Department intended to implement the new personnel system in the summer of 2005, district court decisions in July, August, and October enjoined the Department from implementing significant portions of MAXHR. Whether the Department appeals or proposes further modifications to the program, significant implementation delays are certain. Those delays will impact the cost of implementation, the current development and implementation contract, and the ability to properly and effectively manage its workforce.

We are coordinating with the Government Accountability Office to closely monitor DHS' efforts to create and implement its new human capital management system.

INTEGRATION OF INFORMATION SYSTEMS

Creating a single infrastructure for effective communications and information exchange at various classification levels within the Department remains a major management challenge for DHS. To meet this challenge, the Chief Information Officer (CIO) has outlined an Information Technology Infrastructure Transformation Program to create a secure, sensitive but unclassified network and a common email system for sharing across the Department. The program includes consolidating data centers, as a means of reducing costs and increasing reliability and survivability of the computing environment. Further, the program discusses plans for transforming helpdesk and other related support services. In September 2005, the Transformation Program was under review by the Department's senior leadership.

However, the DHS CIO is not well positioned to accomplish these IT integration objectives. Despite federal laws and requirements, the CIO is not a member of the senior management team with authority to strategically manage Department-wide technology assets and programs. Although steps recently have been taken to formalize reporting relationships between the DHS CIO and the CIOs of major component organizations, the CIO still does not have sufficient staff resources to assist in carrying out the planning, policy formation, and other IT management activities needed to support Departmental units. While the CIO currently participates as an integral member at each level of the investment review process, the Department would benefit from following the successful examples of other Federal agencies in positioning their CIOs with the authority and influence needed to guide executive decisions on Department-wide IT investments and strategies.

SECURITY OF INFORMATION TECHNOLOGY INFRASTRUCTURE

The security of IT infrastructure is a major management challenge. As required by the Federal Information Security Management Act (FISMA), the CIO must develop and implement a Department-wide information security program that ensures the effectiveness of security controls over information resources, including its intelligence systems, which address the risks and vulnerabilities facing DHS' IT systems.

As we reported in September 2005, based upon its annual FISMA evaluation (excluding its intelligence systems), DHS achieved two significant milestones that will help the Department move toward managing a successful information security program. First, DHS completed a comprehensive inventory of its major applications and general support systems for all DHS' components. Second, DHS implemented a Department-wide certification and accreditation (C&A) tool that incorporates the guidance required to adequately complete a C&A for all systems. The completion of these two tasks eliminated two factors that significantly held the Department back in achieving some success in establishing its security program in the last two years.

As we reported in our FY 2004 FISMA evaluation, and despite several major improvements in DHS' information security program, DHS' components have not completely aligned their respective information security programs with DHS' overall policies, procedures, and practices. For example, not all DHS systems have not been certified and accredited. The CIO has developed a detailed remediation plan to accredit all systems by September 2006. In addition, not all components' information security weaknesses are included in their Plan of Action and Milestones nor is the data in the enterprise management tool complete and current. To address this issue, the CIO will identify ways to improve the review process and increase accountability at the components. The CIO has also made numerous upgrades to its management tool, to improve the accuracy and completeness of the data.

The Department is also tasked to protect its national security systems. We reported in January 2005 that DHS needed to take steps to provide adequate security for the information and information systems that support its classified operations and assets. DHS must also ensure the confidentiality, integrity, and availability of vital classified information. DHS concurred with our recommendations.

INFRASTRUCTURE THREAT ASSESSMENT

The Department is tasked to protect the Nation's critical infrastructure and national assets against terrorist attack. Before this assignment can be executed to its fullest, DHS must identify and compile the Nation's critical infrastructure and national assets into a comprehensive National Assets Database (NADB). DHS has made progress on this task; as of July 2004, the NADB contained more than 75,000 national assets. However, the process the DHS is using to assess the threats against those assets, determine how vulnerable they are to attack, ascertain their mitigation requirements, and prioritize the threat/mitigation effort is evolving. Presently, there is no blueprint for the NADB as no precedent exists for collecting such extensive information and making these difficult qualitative and quantitative assessments. Policies and procedures for maintaining the NADB are still in development. Although IAIP provided guidance for the collection of data, the data it received was often inconsistent. We are evaluating the effectiveness and efficiency of the processes that DHS employs to develop and prioritize its inventory of the Nation's key assets.

BORDER SECURITY

A primary mission of the DHS is to reduce America's vulnerability to terrorism by controlling the borders of the United States. This mission is shared by a number of agencies within the Department.

CBP inspects visitors and cargoes at the designated U.S. ports of entry (POE) and is responsible for securing the borders between the POEs. CBP's primary mission is to prevent terrorists and terrorist weapons from entering the United States, while also facilitating the flow of legitimate trade and travel. ICE is the investigative agency that enforces immigration and customs laws within the United States. While CBP's responsibilities focus on activities at POEs and along the borders, ICE's responsibilities focus primarily on enforcement activities related to criminal and administrative violations of the immigration and customs laws of the United States, regardless of where the violation occurs. Additionally, CBP and ICE have employees assigned outside the United States to protect the sovereignty of our borders.

Other DHS components share border security responsibilities. The United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program is responsible for developing and fielding DHS' entry-exit system. It also coordinates the integration of two fingerprint systems: DHS' Automated Biometric Identification System (IDENT) and the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System (IAFIS). Also, the U.S. Citizenship and Immigration Services (USCIS) is responsible for reviewing and approving applications for immigration benefits. While not a law enforcement agency, USCIS plays an integral part in DHS' border security program by ensuring that only eligible aliens receive immigration benefits and identifying cases of immigration benefit fraud and other immigration violations that warrant investigation or removal by ICE.

DHS faces several formidable challenges in securing the Nation's borders. These include the development of an effective, automated entry-exit system (US-VISIT); disruption of alien smuggling operations; identifying, locating, detaining, and removing illegal aliens; fielding effective border surveillance technologies; integrating DHS' IDENT with the FBI's IAFIS fingerprint systems; providing timely, accurate, and complete intelligence to support border security operations; developing effective overseas operations, including improved controls over the Visa Waiver Program and lost and stolen passports; and, reducing the immigration benefit application backlog.

For example, CBP needs to fuse the intelligence gathered with intelligence requirements to accomplish its priority mission. The CBP mission of preventing terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel is critical. Knowing the difference between legitimate trade and travel and terrorists is a challenge that timely intelligence often solves threat to our national security. The ability of CBP to gather and distribute intelligence information to field personnel has a direct effect on security at our borders. Border security also depends on information about terrorists kept on various watch lists. The watch lists are managed by several Federal agencies. Those agencies and DHS need to coordinate access to the lists to ensure valuable information flows through CBP to field personnel on the line.

Control over the northern border is another challenge. The external challenges to CBP's mission of managing, securing, and controlling our northern border include 128 ports of entry, thousands of miles of difficult terrain, large expanses of private property, and numerous lakes. The primary internal challenge to CBP is to ensure adequate resources are available. Resources on the northern border now include aircraft, vehicles, facilities, and officers, agents and specialists. CBP must have sufficient number and type of personnel, equipment, and border infrastructure to achieve their mission on the northern, Canadian, border.

A further challenge for DHS are the difficulties CBP and ICE continue to experience coordinating and integrating their respective operations. More than two years after their creation, CBP and ICE have not come together to form a seamless border enforcement program. Their operations have significant interdependencies that have created conflict between CBP and ICE. Jurisdictional, operational, and communication gaps exist between the two organizations that must be addressed by DHS leadership.

We are continuing to maintain an aggressive audit and inspection program for the Department's border security initiatives to ensure that they are being carried out in an economical, efficient, and effective manner.

TRANSPORTATION SECURITY

Airport Screeners

The Aviation and Transportation Security Act (ATSA), which was enacted as a result of the events of September 11, 2001, mandated that the TSA hire and train thousands of screeners for the Nation's 429 commercial airports by November 19, 2002. As a result, TSA hired 62,000 screeners. Our undercover audit of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not being carried into the sterile areas of heavily used airports and do not enter the checked baggage system. Four areas caused most of the test failures and were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA is enhancing its screener training programs, improving management and supervision of screener activities, and testing new technologies.

Checking for Explosives

TSA has been largely successful in its effort to implement the ATSA requirement that all checked bags be screened by explosives detection systems (EDS). However, deployment of the equipment alone does not ensure effective security. For example, TSA has not installed explosives detection technologies at the checkpoint to screen for explosives on the body. As noted above, TSA is in the process of testing several technologies that include backscatter x-ray, explosives trace portals, and document scanner machines to address concerns regarding detection of explosives on individuals. TSA is currently piloting these technologies at 16 commercial airports to assess the operational effectiveness of the technologies.

We are continuing to monitor TSA's progress regarding these issues as well as reviewing TSA's process for screening air cargo.

Maritime Security

The U.S. Coast Guard is the lead DHS agency for maritime homeland security, and is responsible for developing and implementing a comprehensive National Maritime Transportation Security Plan to deter and respond to transportation security incidents. The marine areas under U.S. jurisdiction cover 3.5 million square miles of ocean, 95,000 miles of coastline, and 26,000 miles of commercial waters serving 361 domestic ports. These activities account for two billion tons and $800 billion of domestic and international freight annually. Approximately 8,000 foreign vessels, manned by 200,000 foreign sailors, make more than 50,000 ship visits to U.S. ports each year.

The Coast Guard faces significant management challenges. The most daunting challenges include restoring the Coast Guard's readiness to perform its legacy missions; implementing the Maritime Transportation Security Act of 2002 (MTSA); maintaining and replacing the Coast Guard's deepwater fleet assets; and developing adequate infrastructure needed to support the Coast Guard's multiple missions.

For example, there is growing concern that the resources being devoted by the Coast Guard to its Deepwater Program is reducing its ability to maintain and re-capitalize shore side infrastructure critical to its legacy and homeland security missions. The Coast Guard occupies more than 21,000 buildings and structures totaling more than 33 million square feet of building space. The estimated replacement value for these shore side assets is $7.5 billion. Based on this value, and recent and projected shore infrastructure acquisition, construction, and improvement (AC&I) funding levels, Coast Guard's recapitalization rate[1] hovers around 200 years. This is in sharp contrast to the Department of Defense's target recapitalization rate for its facilities of 67 years.

[1] Recapitalization rate is the number of years required to regenerate a physical plant – either through replacement or major renovation – at a given level of investment in order to keep the facility modern and relevant in an environment of changing standards and missions.

Other Transportation Modes

While TSA continues to address critical aviation security needs, it is moving slowly to improve security across the other modes of transportation. About 6,000 agencies provide transit services through buses, subways, ferries, and light-rail services to about 14 million Americans. TSA requested $5.6 billion to facilitate its operations in FY06. However, only $32 million (less than 1 percent) of this request is earmarked for surface transportation security.

TRADE OPERATIONS AND SECURITY

Trade Operations and Security is primarily the responsibility of CBP. The Coast Guard and ICE also play important roles in support of this area. In a typical year CBP processes millions of sea containers; semi-tractor trailers; rail cars; millions of tons of bulk cargo; and liquids; such as chemicals, crude oil, and petroleum products. They also process or review all of the personnel associated with moving this cargo across our borders or to our seaports. CBP has the counterbalancing mission of facilitating the legitimate trade so vital to our country and at the same time enforcing the laws associated with trade or border controls. CBP has the challenge of interdicting smuggling and stopping other illegal activities that benefit terrorists and their supporters.

Working with the trade, foreign allies, other DHS components, and other Federal, state and local agencies and organizations, CBP is intent on preventing legitimate commercial cargo from being used by smugglers and terrorists to introduce weapons of mass effect or other contraband into the U.S. CBP has implemented a number of initiatives to accomplish this objective such as the Container Security Initiative (CSI), and Customs-Trade Partnership Against Terrorism (C-TPAT). CSI works with foreign allies and partners to screen and examine containerized cargo at overseas port before it is loaded on ships bound for the U.S. The initiative calls for the increased use of non-intrusive technology to inspect this cargo both overseas and at U.S. ports. Within C-TPAT, CBP works with the trade to develop and implement processes and systems to help secure the supply chain. CBP uses targeting systems to assist in identifying the cargo that represents the highest risk, so that the use of precious and limited resources can be focused on this cargo. Other initiatives include developing a "smart" container that will provide extra protection or warning of tampering or intrusion. In support of CBP's overall trade mission, they are undertaking an extensive and long-term effort to develop a new automated system (ACE) to replace older, less effective and capable trade processing systems. This effort is not scheduled to be fully competed until 2011, and will cost more than $3.3 billion dollars.

We issued a report regarding the Automated Targeting System (ATS) used to help identify high-risk cargo, and other aspects of the environment in which it is used. In this report, we made several observations about the trade supply chain and its vulnerabilities. We concluded that improvements could be made with regard to the data to which ATS targeting rules are applied, that examination results should be used more systematically in developing targeting rules, and that physical controls over containers selected for examination can be improved. As this review is legislatively mandated, we are currently reviewing other aspects of the ATS and its operational environment.

Management's Response to The Office Of The Inspector General's Report On Major Management Challenges Facing The Department Of Homeland Security

The following provides specific responses to those issues raised by the Inspector General's (IG) statement on the top management challenges facing the Department.

DISASTER RESPONSE AND RECOVERY

As highlighted in the IG Statement, the Department recognizes the need for oversight of spending on Katrina recovery efforts. The Department has taken numerous actions to address this issue. In addition to the IG teams now reviewing Katrina and Rita contracts, the Department is establishing a Katrina recovery contracting office to provide a dedicated procurement staff to oversee Katrina recovery contracting work and has formed a fraud, waste and abuse taskforce to ensure the proper financial controls are in place to manage the recovery effort. The Department has brought in outside expertise to conduct tests of FEMA's internal controls and to assess what organizational, staffing and business process changes are necessary for FEMA's financial management organizations to manage the supplemental funding. Dozens of detailees from Department Component CFO organizations have been assigned to FEMA to assist in budget and financial management of the response and recovery work. Secretary Chertoff has communicated to Congress that the Department will ensure that FEMA has mature, solid contracting and procurement systems in place before a disaster – and that those systems include a special focus on procurement integrity.

The Department is taking action to address the IG concern to improve FEMA information technology (IT) systems. During the Katrina response, our efforts were significantly hampered by a lack of information from the ground. With communication systems damaged and state and local assets compromised by the subsequent flooding, our ability to obtain precise reporting was significantly impaired. The sheer force of Hurricane Katrina disabled many of the communications systems that state and local authorities and first responders rely upon to communicate with each other and with FEMA. This was not an issue of interoperability, but of basic operability resulting from wind, flooding, loss of power, and other damage to infrastructure. We are ensuring sufficient communications capabilities are in place in the future and able to function during the worst phases of a hurricane or incident. Future communications must also ensure FEMA has its own increased communications capability so we do not face a similar situation. While satellite phones are helpful, they are not a panacea. We are looking at ways to adapt military and advanced private sector communication technology for emergency use – to help state and local first responders as well as FEMA support personnel.

We are also working to improve other FEMA IT systems related to the business processes for registering people for assistance, and getting them the benefits they need. The Department is evaluating FEMA's disaster registration processes and databases to make sure we have a high degree of confidence in those systems. We want to have the flexibility to use this information to provide a level of granular detail that enables us to make informed decisions about where to focus our attention and resources, and how to better assist our state and local partners.

In response to the OIG's concern regarding the Multi-Year Flood Hazard Plan, FEMA's 5-year budget and schedule plan for flood hazard data development was issued November 2004 and updated June 2005. This plan reflects funding received and anticipated from the President and Congress. FEMA recognizes that this level of funding does not meet all of the needs of our State and local mapping partners; however, it is important to note that FEMA's role in flood map modernization focuses on essential flood mapping requirements and must be complemented by others. A business planning and standards improvement process with stakeholders is in place to facilitate collaboration and coordination on plan improvements. FEMA is currently evaluating the level of funding required for flood map maintenance. A Partnership Building Plan was issued in March 2005 to develop and implement better strategies for partnering with state and local entities with varying levels of capabilities and resources. In addition, FEMA issued a formal policy on geospatial data coordination in August 2005, and established a geospatial data coordination and standardization management team to support the implementation of the policy in cooperation with stakeholders.

CONSOLIDATING THE DEPARTMENT'S COMPONENTS

Proposed changes to the Department of Homeland Security's structure and organization as a result of the Second Stage Review are designed to improve our capabilities to protect and safeguard this nation. One critical need within the Department is to have the capacity to think through broad and overarching issues with a Department-wide perspective, rather than just through the lenses of one particular component. By integrating and coordinating areas of intelligence, policy, operations and preparedness efforts, this Department will be in a stronger position to respond actively to present and future threats with appropriate actions and policies.

In regards to consolidating the Department's components, the IG raised the issue regarding the proposal to merge CBP and ICE. Based on the Second State Review of the entire Department, the Secretary determined that ICE and CBP would not be merged. To address the coordination issues involving intelligence, operations, and policy, the Secretary determined that a reorganization of the Department would best address these coordination issues for the entire Department, including ICE and CBP. New policy, operations, and intelligence directorates are being established to facilitate coordination between all of the Department's components in the areas of policy, operations, and intelligence.

Another issue raised by the IG in this arena was the effectiveness of the dual accountability structure for business operations. The Department has implemented the dual accountability structure during fiscal year 2005, and the system has assisted in the integration and streamlining of support service functions. Creating functional excellence required every executive, manager, and employee in the Department to create an environment that rewards collaboration, promotes best practices, and shares accountability for the performance of the management support systems that enable the Department to fulfill its missions. The concept of dual accountability mandates that both components and key departmental functional experts are responsible for organizational excellences. The department functional experts are held accountable for designing systems to optimize service functions, setting the standards for function performance, creating the department-wide policies and processes, providing the automated solutions to yield greater efficiencies, and nurturing the development and success of centers of excellence. Components are likewise accountable to support these progressive business functions as s key pert of their commitment to mission accomplishment.

In all efforts of this magnitude, when so much is to be gained, the integration and alignment of each function requires strong communication, respect for both individuals and processes, and a shared resolve to finds solutions that benefit both mission accomplishment and functional excellence. Leadership across the Department is challenging traditional approaches, communicating, and executing as a team to design and execute support functions that will constitute progressive 21st century excellence in governance.

CONTRACT MANAGEMENT

While the IG report highlights some ongoing challenges in the contract management arena, there have been improvements since last year in the Department's contract management system. For instance, clear lines of responsibility have been established in this arena. The Undersecretary of Management (USM) is responsible for establishing department-wide policies and procedures for program management operations. Within USM, the CPO has responsibility for the acquisition workforce, acquisition policy, and oversight. The CFO's Program Analysis and Evaluation (PA&E) office is responsible for coordinating reviews for the Investment Review Board and Joint Requirements Council (JRC), which provide Department oversight of major acquisitions.

The Department recognizes that ensuring the necessary numbers of certified program management staff are present is a multi year issue, and is actively working to increase the number of certified program management staff in the Department. The Department currently has an agreement with the Defense Acquisition University for program management training. The Department is instituting improvements to the IRB process, the most notable being implementing an integrated review process to provide decision makers with advice from functional experts (within the CFO, CIO, CPO, CAO, S&T, Policy, General Law & Privacy). The department is also developing procedures for independent verification and validation (IV&V) of major investments, addressing another IG concern. As part of the IRB governance process, additional emphasis is placed on assuring that a program management office is in place on Level I and II initiatives.

The Department concurs with the IG that several high visibility investments in the Department (ACE, US-VISIT, Deepwater) require close management. These investments are reviewed quarterly when they submit their status reports that are required by Congress, along with an intensive review that occurs with submittal for approval of their annual expenditures plans. The Department is working to implement a quarterly reporting process for all major investments that will gauge project management efforts in terms of adherence to cost, schedule, and performance.

To address the staffing disparities in procurement offices, the CPO established target staffing levels and communicated this to Department components in writing. The CPO provided input to the CFO for the fiscal year 2007 to fiscal year 2011 budget to support the target staffing levels.

GRANTS MANAGEMENT

State and Local Government Coordination and Preparedness (SLGCP) has taken a number of steps to address the grants management challenges identified in the IG. First is the establishment of SLGCP's internal grant financial management office, the Office of Grant Operations (OGO). Effective October 1, 2005, OGO assumed responsibility for all pre- and post-award grant financial management activities for the SLGCP programs currently serviced by its legacy Department of Justice organization. The OGO staff has defined its financial monitoring parameters and objectives and is finalizing its fiscal year 2006 monitoring plan and site visit/desk review guidelines. The goal is to ensure that adequate financial monitoring is performed on SLGCP's expanding portfolio of grants. During the month of October 2005, OGO will begin fulfilling monitoring objectives by performing site visits in tandem with program managers from SLGCP's Preparedness Programs Division (PPD). Another step taken to address these management challenges is the establishment of the Transportation Infrastructure Security Division (TISD) within PPD. This Division is staffed by transportation subject matter experts, and was created specifically to manage the transportation-related grant programs inherited from the Transportation Security Administration (TSA).

The second major accomplishment is the use of risk criteria in making grant allocation decisions. Specifically, SLGCP, in coordination with IAIP and the Coast Guard, refined the fiscal year 2005 Port Security Grant Program to make the allocation of funds more risk-based. As part of this process, a risk-based formula was used to limit eligibility to the nation's sixty-six (66) most at-risk ports. In addition, national port security priorities were identified for the program, and the application review process was sharpened to focus on these national priorities, as well as local port security factors like alignment with the port's Area Maritime Security Plan. Based on these program enhancements, the Department's IG concluded that SLGCP had sufficiently responded to the recommendations contained in IG Report 05-10, Review of the Port Security Grant Program, and closed all of the recommendations contained in this report in July, 2005.

At the outset, the Department acknowledges that although we have substantial resources to provide security, these resources are not unlimited. Therefore, we as a nation must make tough choices about how to invest finite human and financial capital to attain the optimal state of preparedness. In making the tough choices on where and how to invest in security, the Department will focus preparedness on objective measures of risk and performance. This risk analysis is based on these three variables: (1) threat; (2) vulnerability; and (3) consequences. These variables are not equal – for example, some infrastructure is quite vulnerable, but the consequences of attack are relatively small; other infrastructure may be much less vulnerable, but the consequences of a successful attack are very high, even catastrophic.

The Department will concentrate first and most relentlessly on addressing threats that pose catastrophic consequences. Some of the tools needed to prevent, respond and recover from such awful scenarios are already in place; but others need significant improvement. The first step in enhancing national preparedness is establishing a preparedness baseline that measures the effectiveness of our planning for preventing, protecting against, and responding to terrorist acts or disasters. A Department review team has, therefore, constructed the model for an analytic matrix that will set that baseline. The matrix will allow us to analyze possible threats and will map the current state of prevention, protection and response planning with regard to each. This matrix will be a critical tool enabling us to identify and remedy current gaps in preparedness.

Bringing greater planning discipline to each of these risk scenarios ensures we secure the highest risk areas, especially in executing our preparedness mission. And simple common sense counsels that we begin by concentrating on events with the greatest potential consequences. That is why the Department's National Preparedness Goal -- and additional, risk-based planning -- will form our standard in allocating future Department grants to our state and local partners so that we build the right capabilities in the right places at the right level. Federal money will be distributed using the risk-based approach that we will apply to all preparedness activities.

FINANCIAL MANAGEMENT

The Department is committed to world-class financial management. The Department continues to proactively monitor the management and oversight of financial management improvements for ICE and Coast Guard as well as other Department components whose deficiencies in internal control compromise the integrity of financial reporting in the department. All Department components have corrective action plans to fix existing material weaknesses identified in the audit to achieve an unqualified audit opinion on the consolidated financial statements. The Department's CFO has instituted a Three Year Vision for Financial Reporting to position the Department for an unqualified opinion on the fiscal year 2007 financial statements. The Department's CFO's Office (OCFO) continues to meet regularly with all the Department components, including Coast Guard and ICE to assess progress against both the correct action plan and CFO's Vision, and to discuss and resolve problem areas.

The OCFO is continuing its efforts to functionally integrate the financial management line of business activities at the Department. The OCFO has already realized progress toward the vision of a unified financial management system for the Department by reducing and consolidating the number of disparate budget, finance, and accounting processes, providers, and systems. Since the Department's inception, OCFO has reduced the number of accounting providers from nineteen to eight. The OCFO is continuing to enhance its guidance to and oversight of Components and is making significant progress in establishing Department-wide standard operating procedures and policies, particularly in the areas of budget execution, financial management, and financial reporting. We will continue to work with the IG as we proceed to improve our financial management practices.

DHS FINANCIAL ACCOUNTABILITY ACT

Fiscal year 2005 proved to be a watershed year for internal controls at the Department of Homeland Security. Shortly after passage of the DHS Financial Accountability Act, the Department developed a strategy and vision for implementation. Most notably, the Department established an Internal Control Committee (ICC) responsible for improving internal controls. ICC membership includes a Senior Management Council, ICC Board, and Senior Assessment Team. The Senior Management Council is comprised of the Department's Under Secretary for Management, CAO, CFO, CHCO, CIO, and CPO. Their function entails overall management accountability, monitoring of corrective action plans, and ICC sponsorship. The ICC Board seeks to integrate and coordinate internal control assessments with other internal control-related activities and includes representatives from all Department lines of business to address crosscutting internal control challenges. Finally, the Senior Assessment Team comprised of senior level financial managers carries out and directs Component level internal control assessments. Over the past year the ICC has:

- Published our landmark implementation guide, which is specifically tailored to support an attestation on internal control over financial reporting as required by the DHS Financial Accountability Act.
- Developed a comprehensive integrated framework for the Federal Financial Managers' Financial Integrity Act and have taken significant steps to prepare for implementing the recent revisions to OMB Circular A-123, Management's Responsibility for Internal Control, effective in fiscal year 2006.
- Implemented the GAO Internal Control Management and Evaluation Tool across the Department to facilitate the development of internal control activities in accordance with GAO's Standards for Internal Control in the Federal Government.
- Initiated a seven-step plan to prepare for the fiscal year 2006 audit of internal controls over financial reporting.
- Completed a comprehensive internal control assessment of the consolidated financial reporting process within the OCFO. In addition, the Coast Guard, one of our largest Components, has initiated process level documentation pilots.
- Developed corrective action plans for all material weaknesses and reportable conditions and a Management Directive and Process Guide to ensure these corrective action plans demonstrate results.

HUMAN CAPITAL MANAGEMENT

While the District court decisions have enjoined the Department from implementing certain portions of MAXHR, the classification, pay and performance management provisions of the new human resources management program are moving forward. Deployment of the new performance management system is being implemented for covered employees, including managers, supervisors, non bargaining unit employees, in Headquarters starting in October 2005, and will be expanded during fiscal year 2006 to other Department components, such as FLETC, Secret Service, USCG, FEMA and ICE. Significant design work will continue on the new pay system with planned implementation by January 2007 for phase 1 organizations, such as HQs, Secret Service, USCG, FEMA and FLETC. Emphasis on performance management training for all audiences, i.e., managers, supervisors, HR specialists, systems administrators, and all employees, will continue throughout fiscal year 2006. The Department also evaluated the impact on the fiscal year 2006 funding requirement and reduced the request accordingly. It is anticipated that the overall cost for full implementation will not increase.

INTEGRATION OF INFORMATION SYSTEMS

CIO believes it is properly positioned and has the authority it needs to accomplish its mission. The CIO is the principal IT authority to the Secretary and Deputy Secretary, and it will continue to hold that leadership role within the Department. The CIO continues to work on the integration of its information systems. To that end, the Infrastructure Transformation Office (ITP) has been tasked with improving information sharing and interoperability, providing a reliable and scalable infrastructure, and managing costs efficiently. To effectively manage this transformation from over 20 individual, stand-alone IT infrastructures with minimal interconnectivity, to a single, cohesive IT infrastructure, the ITP is organized by the following project areas:

- Network Services: Establish an integrated enterprise network for the Department by streamlining and standardizing the network environment, minimizing the amount of redundant IT infrastructure, providing operational and security support, and developing a Department-wide network topology with centralized governance and standardized procedures.
- Email Services: Establish a common, SBU e-mail system for the Department and provide enterprise directory services.
- Help Desk and Related Services: Establish a centralized help desk capability to resolve issues such as network connectivity, data access, and email access.
- Data Center Services: Establish two data center facilities that will improve information availability by standardizing backup functionality, improve security by reducing the number of locations and consolidating network entry points, improve system reliability by employing enhanced environmentals, and improve the real-time availability of Department data.
- Video Services: Establish a standard, enterprise-wide video operations capability for the Department.

SECURITY OF INFORMATION TECHNOLOGY INFRASTRUCTURE

The success of the Department's mission is absolutely dependent on our ability to protect sensitive information used in defending the homeland. While much of the Information Security Program is structured around compliance with FISMA, OMB and National Institute of Standards and Technology (NIST) standards and guidance, the Department's Information Security Program has also been designed to provide a secure and trusted computing environment based on sound, risk-management principles and program planning.

We agree that compliance on the part of the Department component organizations is paramount to the success of a Departmental information security plan. To this end, the Office of the CIO recently completed a comprehensive inventory of all information systems currently in use within the components, as well as in the headquarters organizations. This inventory followed a common methodology for determining appropriate security boundaries and will now serve as the baseline for systematically improving our systems security. This framework of common inventory definitions, coupled with recently deployed enterprise-wide security management tools and processes, will provide the common trust environment that is necessary for negotiating effective and appropriate rules-of-behavior across system boundaries, thereby facilitating information sharing.

INFRASTRUCTURE THREAT ASSESSMENT

The IG raised concern about the Department's ability to gather information for the National Asset Database (NADB). As of August 2005, the NADB contained nearly 100,000 assets with tens of thousands of other assets available for inclusion. It is important to note that the process of assessing threats against the assets, determining the vulnerability of an asset, and prioritizing the threat mitigation effort is inexorably tied to the data collection effort itself. Data collection is a challenge as Information Protection relies on a myriad of sources for data, and is without a preexisting legal or regulatory framework for data collection or prioritization of information. The Department has been successful in building the needed capabilities, and results are now beginning to emerge. While there is no precedent for collecting the extensive information that forms the NADB, IAIP is leading the way and has created a blueprint for collecting the information and conducting the analysis.

BORDER SECURITY

We agree with the OIG's assessment that the Department faces several formidable challenges in securing the nation's borders. The Department is aggressively addressing these issues and the solutions will require dedicated management oversight. We have developed a comprehensive multi-year plan to secure America's borders and reduce illegal immigration, referred to as the Secure Border Initiative (SBI). To facilitate implementation of SBI, the Department is establishing a program office at the department level to coordinate and integrate policy, provide procurement oversight, and facilitate inter-agency participation for this border and interior enforcement initiative. This includes coordinating and integrating CBP and ICE efforts to form a more seamless border security program. Since resources are not infinite, this program will use a risk based approach to deploy personnel, technology and border infrastructure at both the northern and southern borders.

We will address all aspects of the border security problem across the board – deterrence, detection, response, apprehension, detention, and removal. We will address the challenges in each of these areas with an integrated mix of increased staffing, more robust interior enforcement, greater investment in detection technology and infrastructure, and enhanced coordination on federal, state, local, and international levels. The Department has already made improvements to secure our borders and enforce immigration laws since 9/11. The Department has over 11,000 Border Patrol agents along more than 6,000 miles of northern and southern border, an increase of 15% over 9/11 levels, and is currently adding 1,500 more Border Patrol Agents. An additional 18,000 officers are posted at our Ports of Entry (POE), and over 8,000 agents and officers working to apprehend criminals, absconders, and other individuals illegally in the United States. Despite our substantial progress, we still face a substantial problem. The ability of individuals to enter our country outside legal channels is a threat to our homeland security. Flagrant violation of our borders undercuts the rule of law, undermines our security, and imposes particular economic strains on our border communities.

SBI is designed to enable the Department to achieve operational control of both the northern and southern border within five years. Key elements of SBI include:

- More agents to patrol our borders, secure our ports of entry and enforce immigration laws.
- Expanded and more efficient detention and removal capabilities to eliminate "catch and release" once and for all.
- A comprehensive and systemic upgrading of the technology used in patrolling the border, including increased manned aerial assets, expanded use of UAVs, and next-generation detection technology.
- Increased investment in infrastructure improvements at the border – providing additional physical security to sharply reduce illegal border crossings.
- Greatly increased interior enforcement of our immigration laws – including more robust worksite enforcement.

In response to other Border Security concerns raised by the IG, US-VISIT continues to be a top priority for the Department. US-VISIT entry procedures are currently in place at 115 airports, 15 seaports and in the secondary inspection areas of the 50 busiest land ports of entry. US-VISIT exit procedures are operating at 12 airports and two seaports. Entry procedures will be deployed to the remaining land ports of entry by December 31, 2005.

Efforts to integrate the Department's Automated Biometric identification System (IDENT) system with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) fingerprint system are moving forward. DHS is implementing a plan to transition to 10-print finger print capture in collaboration with Commerce, State, Defense, Justice and State Departments. Immediate 10-print transition efforts will be focused on enrollment efforts, and an initial IDENT/IAFIS interoperability solution is planned within 6 months of this transition. The plan proposes to:

- Begin enrolling foreign nationals using 10-print, while conducting current background checks
- Push aggressive investment to drive biometric technology market to deliver scanning equipment capability
- Improve IDENT to improve accuracy and watch list matching
- Continue to support IDENT/IAFIS interoperability work

To strengthen document integrity, the Department is now requiring a digital photograph of the passport holder's face printed on the data page of the passport after extensive consultation with Congress and the Department of State. The Department imposed an October 26, 2006 deadline for the integrated circuit chip, or e-passport, capable of storing the biographic information from the data page, a digitized photograph, and other biometric information in travel documents. Valid passports issued before October 26, 2005, will still be accepted for travel under the auspices of the Visa Waiver Program (VWP), provided that the passports are machine-readable.

In addition to the digital photo and chip requirements, the Department is taking steps to strengthen document integrity by requiring VWP countries to commit to several measures concerning lost and stolen passports. Among them, the Department will require VWP countries to report all lost and stolen passports to INTERPOL and to the Department, and increase information sharing between VWP countries and the United States government on trends and analysis of lost and stolen passports.

In response to another issue raised by the IG, the Department is committed to reducing the backlog of immigration cases. The goal is to reduce the cycle time for all cases to six months or less. Significant productivity gains must be realized to meet the target of a six-month cycle time for all immigration benefit applications by the end of fiscal year 2006. As such, USCIS is reengineering business processes, increasing the use of information technology to achieve greater efficiencies, updating policies and procedures to increase uniformity of decision making within the adjudication process, managing against milestones, and working cooperatively with stakeholders to identify other means of improvement. USCIS also will intensify its anti-fraud efforts, enhance its quality program, and modernize its information technology systems that will be the backbone of reengineered business processes. The combination of these efforts will ensure we reduce the backlog.

TRANSPORTATION SECURITY

AIRPORT SCREENERS

A Department IG undercover audit of screener performance revealed that improvements are needed in the screening process to ensure that dangerous prohibited items are not introduced into the sterile areas of airports and that explosives, do not enter the checked-baggage system. Four areas caused most of the test failures and were in need of improvement: training; equipment and technology; policy and procedures; and management and supervision. TSA is enhancing its screener training programs, improving management and supervision of screener activities, and testing new technologies.

CHECKING FOR EXPLOSIVES

TSA has been largely successful in its effort to implement the ATSA requirement that all checked bags be screened by explosives-detection systems (EDS). TSA has also deployed technologies, including explosives trace detection (ETD) devices, to detect potential explosives in carry-on baggage. However, deployment of the equipment does not ensure effective security; resolution of technology alarms is a key element to effective security. In the area of checkpoint technology, TSA has installed table top explosives trace detection technologies at the checkpoint to provide some capabilities when screening suspect carry-on items, electronic items, shoes, etc. To increase and automate these capabilities at the checkpoint, TSA has tested several technologies that include explosives detection trace portals and explosives detection document scanners to address detection of explosives on individuals. Based on the results of these pilots, TSA is now deploying the portals to the nation's largest airports. The document scanner that was piloted, while effective, was not determined to be efficient, therefore; TSA has reengaged technology manufacturers to develop an automated document scanner that will provide efficiencies and effectiveness. TSA is also planning to pilot other emerging technologies in fiscal year 2006, to include an automated explosives detection system for carry-on baggage to replace standard x-ray technology, and whole body imaging technology (x-ray backscatter) for screening persons for both weapons and explosives.

MARITIME SECURITY

The United States Coast Guard has been diligent in its mission to provide the nation with maritime security. They are meeting their challenges through a myriad of initiatives including:

- On-going delivery of the Integrated Deepwater System (IDS) including: construction of the first two Maritime Security Cutters-Large to be delivered in fiscal years 2007 and 2008, initial design of the Maritime Patrol Coastal (WPC) and the Maritime
- Security Cutter-Medium; production of the first two Maritime Patrol Aircraft and two Vertical Unmanned Aerial Vehicle (VUAV) to be delivered in fiscal year 2006; continued development of a Common Operating Picture at shore-based Command Centers, an Integrated Logistics Support System and legacy sustainment/enhancement projects for all major cutters and aircraft, including continued re-engineering of the HH-65 short-range helicopter fleet.
- Implementation of the Maritime Transportation Security Act (MTSA) of 2002: In fiscal year 2005 the USCG added 500 personnel to develop, review, and approve approximately 9,000 domestic vessel security plans and 3,200 domestic facility plans; develop 48 Area Maritime Security Plans and Committees; perform 55 domestic Port Security Assessments; develop a national Maritime Transportation Security Plan, verify security plan implementation on 8,100 foreign vessels and continue conducting foreign port security assessments on 100+ countries conducting direct trade with U.S.
- Continuation of the Great Lakes Icebreaker (GLIB) project, which will reach full operating capability in fiscal year 2006.
- Continuation of the Rescue 21 project, recapitalizing the USCG's coastal zone communications network, to ensure completion by the end of fiscal year 2007.
- Adding nearly 100 new personnel to support planning and coordination of all USCG mission at Command Centers.
- Continue implementation of the nationwide Automatic Identification System (AIS), significantly enhancing Maritime Domain Awareness (MDA) and improving the USCG's ability to detect maritime security threats farther from the nation's ports.
- Procurement of new Response Boats: Continue recapitalization of the USCG's obsolete, non-standard utility boats and increase the USCG's presence in critical ports and coastal zones.
- Commence Airborne Use of Force (AUF) implementation on the USCG's entire fleet of helicopters by arming existing helicopters at various Air Stations. AUF capability will improve performance of all homeland security missions, including enhanced protection of U.S. ports.
- Continue C-130J Maritime Patrol Aircraft (MPA) missionization. This project will provide additional MPA resources, enhancing MDA and resulting in increased ability to detect, identify, and monitor maritime security threats such as illegal drug traffickers. Armed with MPA surveillance information, USCG operational commanders can optimize use of surface assets and rotary wing aircraft through targeted interdiction of known threats.

- Added 55 billets for enhancing intelligence collection and oversight as a member of the national Intelligence Community. The staff will support critical maritime intelligence support nodes, the USCG Central Adjudication Facility (CGCAF) at the Security Center in Chesapeake, Va., and program management at the strategic-level.

OTHER TRANSPORTATION MODES

In addition to aviation security, TSA is tasked with managing the security risk to the U.S. surface transportation systems while ensuring the freedom of movement of people and commerce. These systems include nine billion passenger trips per year on the nation's mass transit systems, over 161,000 miles of interstate and national highways and their integrated bridges and tunnels, and nearly 800,000 shipments of hazardous materials (95 percent by truck). For these systems, TSA will address these security responsibilities in partnership with other components of the Department as well as the DOT and other Departments.

TSA has provided the top 10 mass transit and passenger rail agencies with TSA-certified explosives detection canine teams to aid in the identification of explosives materials within the mass transit/rail transportation system. In addition, TSA has hired and deployed 100 surface transportation (rail) inspectors to enhance the level of national transportation security by leveraging private and public partnerships through a consistent national program of compliance reviews, audits, and enforcement actions pertaining to required standards and directives. TSA has implemented computer security and tools to ensure that risk and vulnerability assessments are performed leading to full certification and accreditation of major application and general support systems and to provide a Computer Security Incident Response Capability.

TRADE OPERATIONS AND SECURITY

The Department has developed a multi-layered approach to ensure the safety and security of our trade operations, including several efforts focused on container and supply chain security, namely the Container Security Initiative (CSI), the Customs Trade Partnership Against Terrorism (C-TPAT), and the Automated Targeting System (ATS). In post-9/11 America, CSI is based on an idea that makes sense: extend our zone of security outward so that American borders are the last line of defense, not the first. Through CSI, maritime containers that pose a risk for terrorism are identified and examined at foreign ports before they are shipped to the United States. Early on, CSI focused on implementing the program at the top 20 foreign ports which ship approximately two thirds of the volume of containers to the U.S. Governments from these 20 foreign ports have already agreed to implement CSI. As CSI has evolved, CBP hopes to expand the program to additional ports based on volume, location and strategic concerns. Strong support from countries on the European, Asian and African continents ensure that CSI will continue to expand to ports in those areas.

Since October 2004, CBP and the trade community have worked collaboratively to develop minimum security criteria for importers either already enrolled in the C-TPAT program, or wishing to join this voluntary supply chain security program. These new minimum security criteria help solidify membership expectations, and more clearly define and establish the baseline level of security measures which must be employed by member importers. These security criteria are effective as of March 25, 2005. A phased implementation schedule has been implemented and applies to all C-TPAT Importer members. ATS is an aggressive, sophisticated targeting tool that enhances Customs ability to perform enforcement operations. ATS is a system that will assist Customs officers in identifying imports which pose a high risk of containing narcotics or other contraband. The system standardizes bill-of-lading, entry, and entry summary data received from the Automated Commercial System (ACS) and creates integrated records called "shipments". These shipments are then evaluated and scored by ATS, through the use of over 300 weighted rules derived from targeting methods used by experienced Customs personnel. The higher the score, the more the shipment warrants attention. The system allows inspectors to concentrate on higher-risk shipments for further screening and examination. It provides inspectional personnel with the ability to conduct quick data analysis of profile information accumulated on shippers, carriers and importers. ATS is operating in Newark, NJ, Laredo, TX, Seattle, WA, and the Port of Los Angeles/Long Beach, California. Future plans include the installation of ATS at all major seaports, airports, and land border ports of entry. It may also be expanded to outbound operations to target export cargo for anti-terrorism, currency smuggling, and other export violations.

This Page Left Intentionally Blank